

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

45

Applicant: Yuji TSUKAMOTO, et al.  
Title: CONTENT RENTAL SYSTEM  
Appl. No.: Unassigned  
Filing Date: May 9, 2001  
Examiner: Unassigned  
Art Unit: Unassigned



**CLAIM FOR CONVENTION PRIORITY**

Commissioner for Patents  
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign applications filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

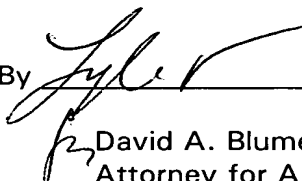
In support of this claim, filed herewith are certified copies of said original foreign applications:

Japanese Patent Application Nos.  
2000-139115 filed 11 May 2000 and  
2001-013815 filed 1 January 2001.

Respectfully submitted,

Date: May 9, 2001

FOLEY & LARDNER  
Washington Harbour  
3000 K Street, N.W., Suite 500  
Washington, D.C. 20007-5109  
Telephone: (202) 672-5407  
Facsimile: (202) 672-5399

By  LYLE KIMMS  
REG. NO. 34079  
David A. Blumenthal  
Attorney for Applicant  
Registration No. 26,257

## 日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENTUS  
45

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2001年 1月22日

出 願 番 号

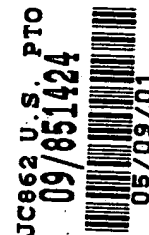
Application Number:

特願2001-013815

出 願 人

Applicant (s):

日本電気株式会社

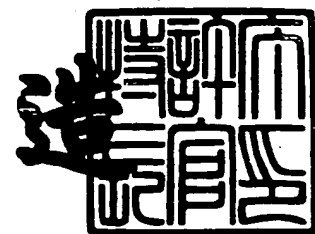


CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 2月16日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2001-3008591

【書類名】 特許願

【整理番号】 34803545

【提出日】 平成13年 1月22日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00  
G06F 17/60

【発明の名称】 コンテンツレンタルシステム

【請求項の数】 19

【発明者】

    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

    【氏名】 塚本 雄二

【発明者】

    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

    【氏名】 辻澤 隆彦

【発明者】

    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

    【氏名】 石川 潤

【発明者】

    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

    【氏名】 吉川 恭史

【発明者】

    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

    【氏名】 山本 克昭

【発明者】

    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

    【氏名】 山川 聡

【特許出願人】

    【識別番号】 000004237

    【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100108578

【弁理士】

【氏名又は名称】 高橋 詔男

【代理人】

【識別番号】 100064908

【弁理士】

【氏名又は名称】 志賀 正武

【選任した代理人】

【識別番号】 100101465

【弁理士】

【氏名又は名称】 青山 正和

【選任した代理人】

【識別番号】 100108453

【弁理士】

【氏名又は名称】 村山 靖彦

【先の出願に基づく優先権主張】

【出願番号】 特願2000-139115

【出願日】 平成12年 5月11日

【手数料の表示】

【予納台帳番号】 008707

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9709418

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツレンタルシステム

【特許請求の範囲】

【請求項 1】 コンテンツを製作するコンテンツ製作所と、

貸し出し事業者が管理する店舗内に設けられたレンタル用サーバであって、前記コンテンツ製作所において作製されたコンテンツが記録され、該記録されたコンテンツが顧客の指定に応じて記録媒体にダウンロードされるレンタル用サーバと、

前記顧客の家に設けられ、前記記録媒体内のコンテンツを再生する再生装置と

からなることを特徴とするコンテンツレンタルシステム。

【請求項 2】 前記貸し出し事業者は、前記記録媒体に前記コンテンツと共に広告映像を記録することを特徴とする請求項 1 に記載のコンテンツレンタルシステム。

【請求項 3】 前記再生装置は前記広告映像に含まれるアイコンがクリックされた時インターネットを介して広告サーバに接続されることを特徴とする請求項 2 に記載のコンテンツレンタルシステム。

【請求項 4】 前記記録媒体は、暗号化されたコンテンツが格納されるコンテンツ格納部と、前記コンテンツを復号する復号鍵が記憶されるメモリと、前記メモリをバックアップするコンデンサとを具備し、前記コンデンサは前記レンタル用サーバによって充電されることを特徴とする請求項 1 ～請求項 3 のいずれかの項に記載のコンテンツレンタルシステム。

【請求項 5】 前記記録媒体は、コンテンツが格納されるコンテンツ格納部と、前記コンテンツを読み出す制御アルゴリズムが記憶されるメモリと、前記メモリをバックアップするコンデンサとを具備し、前記コンデンサは前記レンタル用サーバによって充電されることを特徴とする請求項 1 ～請求項 3 のいずれかの項に記載のコンテンツレンタルシステム。

【請求項 6】 前記記録媒体は、暗号化されたコンテンツが格納されるコンテンツ格納部と、前記コンテンツを復号する復号鍵が記憶されるメモリと、記録

媒体が前記レンタル用サーバに接続されてから一定時間経過後に前記メモリ内のデータを消去するタイマとを具備することを特徴とする請求項 1 ～請求項 3 のいずれかの項に記載のコンテンツレンタルシステム。

【請求項 7】 前記記録媒体は、コンテンツが格納されるコンテンツ格納部と、前記コンテンツを読み出す制御アルゴリズムが記憶されるメモリと、記録媒体が前記レンタル用サーバに接続されてから一定時間経過後に前記メモリ内のデータを消去するタイマとを具備することを特徴とする請求項 1 ～請求項 3 のいずれかの項に記載のコンテンツレンタルシステム。

【請求項 8】 前記レンタル用サーバによって充電され、前記タイマへ電源を供給するコンデンサを設けたことを特徴とする請求項 6 または請求項 7 に記載のコンテンツレンタルシステム。

【請求項 9】 顧客が所持する記憶媒体にコンテンツがダウンロードされ、前記顧客が所持する IC カード内のデータに基づいて前記コンテンツのセキュリティ管理が行われるコンテンツレンタルシステムにおいて、

前記コンテンツを製作するコンテンツ製作所と、

前記コンテンツ製作所において作製されたコンテンツを複数の貸し出し事業者へ配信する管理センタと、

前記貸し出し事業者が管理する店舗内に設けられたレンタル用サーバであって、前記管理センタから配信されたコンテンツが記録され、該記録されたコンテンツを前記顧客の指定に応じて前記記録媒体にダウンロードすると共に、前記 IC カード内のデータに基づいて前記コンテンツのセキュリティを管理するレンタル用サーバと、

前記顧客の家に設けられ、前記記録媒体内のコンテンツを再生すると共に、前記 IC カード内のデータに基づいて前記コンテンツのセキュリティを管理する再生装置と、

からなることを特徴とするコンテンツレンタルシステム。

【請求項 10】 前記 IC カードが前記再生装置にセットされた時、前記再生装置が IC カードの認証を行い、前記 IC カードが前記再生装置の認証を行うことを特徴とする請求項 9 に記載のコンテンツレンタルシステム。

【請求項 1 1】 前記再生装置の認証は、前記再生装置が再生装置公開鍵証明書を前記 I C カードへ送信し、前記 I C カードが該再生装置公開鍵証明書を認証する処理であり、前記 I C カードの認証は、前記 I C カードが I C カード公開鍵証明書を前記再生装置へ送信し、前記再生装置が該 I C カード公開鍵証明書を認証する処理であることを特徴とする請求項 1 0 に記載のコンテンツレンタルシステム。

【請求項 1 2】 前記再生装置の認証は、前記 I C カードが乱数を再生装置公開鍵によって暗号化して再生装置へ送信し、前記再生装置が前記暗号化された乱数を再生装置秘密鍵によって復号して前記 I C カードへ送信し、前記 I C カードがその復号化された乱数に基づいて認証することを特徴とする請求項 1 0 に記載のコンテンツレンタルシステム。

【請求項 1 3】 前記 I C カードの認証は、前記再生装置が乱数を I C カード公開鍵によって暗号化して I C カードへ送信し、前記 I C カードが前記暗号化された乱数を I C カード秘密鍵によって復号して前記再生装置へ送信し、前記再生装置がその復号化された乱数に基づいて認証することを特徴とする請求項 1 0 に記載のコンテンツレンタルシステム。

【請求項 1 4】 前記 I C カードが前記レンタル用サーバにセットされた時、前記レンタル用サーバが前記管理センタと協働で I C カードの認証を行うことを特徴とする請求項 9 に記載のコンテンツレンタルシステム。

【請求項 1 5】 前記 I C カードの認証は、前記 I C カードが I C カード公開鍵証明書を前記レンタル用サーバを介して前記管理センタへ送信し、前記管理センタが該 I C カード公開鍵証明書を認証する処理であることを特徴とする請求項 1 4 に記載のコンテンツレンタルシステム。

【請求項 1 6】 前記 I C カードの認証は、前記管理センタが乱数を I C カード公開鍵によって暗号化して前記レンタル用サーバを介して I C カードへ送信し、前記 I C カードが前記暗号化された乱数を I C カード秘密鍵によって復号して前記レンタル用サーバを介して管理センタへ送信し、前記管理センタがその復号化された乱数に基づいて認証することを特徴とする請求項 1 4 に記載のコンテンツレンタルシステム。

【請求項 1 7】 前記 I C カードが前記レンタル用サーバにセットされた時、前記 I C カードが再生装置公開鍵証明書の前記レンタル用サーバを介して前記管理センタへ送信し、前記管理センタが該再生装置公開鍵証明書に基づいて再生装置の認証を行うことを特徴とする請求項 1 4 に記載のコンテンツレンタルシステム。

【請求項 1 8】 前記レンタル用サーバは、前記記憶媒体および I C カードがセットされ、前記顧客がコンテンツを選択した時、契約内容を前記 I C カードへ送信し、

前記 I C カードが前記契約内容を暗号化して前記レンタル用サーバを介して前記管理センタへ送信し、

前記管理センタが前記契約内容を復号し認証した後前記顧客が選択したコンテンツの暗号鍵を暗号化して前記レンタル用サーバを介して前記 I C カードへ送信し、

前記 I C カードが前記コンテンツの暗号鍵を復号して認証した後、前記レンタル用サーバへ正常通知を行い、

前記レンタル用サーバが前記正常通知を受け、コンテンツを前記記憶媒体にダウンロードすることを特徴とする請求項 9 に記載のコンテンツレンタルシステム。

【請求項 1 9】 前記再生装置は、前記記憶媒体および前記 I C カードがセットされた時、前記 I C カードへコンテンツ暗号鍵送信要求を行い、

前記 I C カードが該送信要求を受け、コンテンツ暗号鍵を暗号化して前記再生装置へ送信し、

前記再生装置が前記暗号化されたコンテンツ暗号鍵を復号し認証した後、復号したコンテンツ暗号鍵を用いて前記コンテンツを再生することを特徴とする請求項 9 に記載のコンテンツレンタルシステム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、映画、放映済みテレビ番組、レッスンビデオ等のコンテンツを有



料でレンタルするコンテンツレンタルシステムに関する。

【 0 0 0 2 】

【従来の技術】

従来のビデオソフトのレンタルシステムの概略構成を図 3 0 に示す。この図において、映像製作会社 1 とビデオソフトメーカー 6 は、ビデオソフトの頒布権行使委託契約 1 5 を締結する。映像製作会社 1 からビデオソフトメーカー 6 にはビデオソフト作成用のマスターテープがマスターテープ供給 1 7 として配布され、そのマスターをもとに、ビデオソフトメーカー 6 は複数の貸し出し用ビデオソフトを作成する。また、ビデオソフトメーカー 6 は、マスターテープの供給 1 7 の対価として映像製作会社 1 に使用料金支払い 1 6 を行う。なお、この貸し出し用ビデオソフトとしては、現在主に磁気テープが用いられており、一部レーザーディスクや DVD-ROM 等の読み出し専用光ディスクも用いられている。

【 0 0 0 3 】

ビデオソフトメーカー 6 と貸し出し事業者 3 との間には中間流通業者として卸業者 7 が存在する。ビデオソフトメーカー 6 からは貸し出し用ビデオソフト等の貸し出し用備品 6 1 が卸業者 7 を介して貸出用備品の供給 7 1 として貸し出し事業者 3 に供給される。一方、卸業者 7 からビデオソフトメーカー 6 には使用料金支払い 6 2 が行われる。また、貸し出し事業者 3 から卸業者 7 にはビデオソフトの購入代金支払い 7 2 が行われ、その際、本数が報告される。なお、中間流通業者として卸業者 7 が存在しない、直接販売契約も存在する。

【 0 0 0 4 】

また、ビデオソフトの著作権使用料等の徴収に関わる使用料徴収委託契約 5 1 がビデオソフトメーカー 6 と各種著作権協会 5 との間で締結されており、ビデオソフトメーカー 6 から各種著作権協会 5 へ著作権使用料支払 5 2 が行われる。

【 0 0 0 5 】

著作権等の使用許諾契約に関しては、図 3 1 に示すように、ビデオソフトメーカー 6 と貸し出し事業者 3 との間に、頒布権委託協会（例えば、特殊法人である（社）日本映像ソフト協会） 8 が存在し、ビデオソフトメーカー 6 と頒布権委託協会 8 の間に頒布権行使委託契約 6 4 が結ばれる。また、貸し出し事業者 3 から

頒布権委託協会 8 にレンタル許諾のための許諾申請書の提出 8 1 を行い、許諾が認められたら頒布権委託協会 8 から貸し出し事業者 3 に加盟店プレート交付 8 3 が行われる。この交付とともに、頒布権委託協会 8 と貸し出し事業者 3 との間に貸し出し業務許諾契約 8 4 が結ばれ、貸し出し事業者 3 と各種著作権協会 5 との間にも貸し出し業務許諾契約 8 4 が結ばれ、著作権使用料がシステム加入料支払い 8 1 として支払い、頒布権委託協会 8 を通して各種著作権協会へ支払われる場合もある。

## 【0006】

## 【発明が解決しようとする課題】

以上のような、従来のビデオソフトレンタルシステムには、次のような状況と問題点がある。

(1) 貸し出し事業者がビデオソフトを購入する場合に、需要の度合いを考慮して、予め同時にレンタルされる本数やレンタル回転率をある程度正確に予測する必要がある。この予測が不正確で必要よりも多くビデオソフトを購入した場合には、貸し出し事業者は不良在庫を抱えることになる。逆に、予測を越えたレンタル希望数があった場合には、顧客が借りたくても、ビデオソフトが店頭に無いという機会損失を招くことになる。

## 【0007】

(2) 前述した状況 (1) はビデオソフトメーカーにとっても、同様であり、マスターテープから作成する貸し出し用磁気テープの本数が問題である。例えば、貸し出し回転率の悪いビデオソフトは、価格を下げて販売用のセルビデオとして中古市場に流出するため、セルビデオソフトの価格も同時に低下する。

## 【0008】

(3) 磁気テープを用いた従来のビデオソフトには、番組の冒頭または終了後に映像製作会社が今後新たに製作する映画や、新たに販売を開始するビデオソフトの CM が挿入されていることが多い。この CM 挿入、すなわち広告収入によりビデオソフトの価格を低く抑えることができるという利点があるが、レンタル開始後時間が経過したビデオソフトでは、CM 効果が得られないばかりか、新着ビデオに関して、視聴者に混乱を招く場合もある。

【 0 0 0 9 】

(4) 流通システムの問題ではないが、磁気テープはレンタル回数を重ねる毎に画像品質が悪化すること、顧客にとって不利益であり、レンタルビデオ視聴中にトラッキング不良等により、ノイズ発生や視聴不能状態に陥る場合がある。

(5) ビデオソフトの不正コピーの流出が、従来から指摘されており、映像ソフトがデジタル化すると、不正コピーの出現は、映像製作会社やビデオソフトメーカーの経営をゆるがす致命的な問題となる。

【 0 0 1 0 】

この発明は、このような事情を考慮してなされたもので、その目的は、貸出業者において不良在庫や機会喪失の虞れがなく、また、セルビデオソフトの価格を低下させる虞れがなく、また、常に最新のCMを挿入することができ、さらに、不正コピーを防止することができるコンテンツレンタルシステムを提供することにある。

【 0 0 1 1 】

【課題を解決するための手段】

この発明は上記の課題を解決すべくなされたもので、請求項1に記載の発明は、コンテンツを製作するコンテンツ製作所と、貸し出し事業者が管理する店舗内に設けられたレンタル用サーバであって、前記コンテンツ製作所において作製されたコンテンツが記録され、該記録されたコンテンツが顧客の指定に応じて記録媒体にダウンロードされるレンタル用サーバと、前記顧客の家に設けられ、前記記録媒体内のコンテンツを再生する再生装置とからなることを特徴とするコンテンツレンタルシステムである。

【 0 0 1 2 】

請求項2に記載の発明は、請求項1に記載のコンテンツレンタルシステムにおいて、前記貸し出し事業者は、前記記録媒体に前記コンテンツと共に広告映像を記録することを特徴とする。

請求項3に記載の発明は、請求項2に記載のコンテンツレンタルシステムにおいて、前記再生装置は前記広告映像に含まれるアイコンがクリックされた時インターネットを介して広告サーバに接続されることを特徴とする。

請求項 4 に記載の発明は、請求項 1 ～請求項 3 のいずれかの項に記載のコンテンツレンタルシステムにおいて、前記記録媒体は、暗号化されたコンテンツが格納されるコンテンツ格納部と、前記コンテンツを復号する復号鍵が記憶されるメモリと、前記メモリをバックアップするコンデンサとを具備し、前記コンデンサは前記レンタル用サーバによって充電されることを特徴とする。

## 【 0 0 1 3 】

請求項 5 に記載の発明は、請求項 1 ～請求項 3 のいずれかの項に記載のコンテンツレンタルシステムにおいて、前記記録媒体は、コンテンツが格納されるコンテンツ格納部と、前記コンテンツを読み出す制御アルゴリズムが記憶されるメモリと、前記メモリをバックアップするコンデンサとを具備し、前記コンデンサは前記レンタル用サーバによって充電されることを特徴とする。

請求項 6 に記載の発明は、請求項 1 ～請求項 3 のいずれかの項に記載のコンテンツレンタルシステムにおいて、前記記録媒体は、暗号化されたコンテンツが格納されるコンテンツ格納部と、前記コンテンツを復号する復号鍵が記憶されるメモリと、記録媒体が前記レンタル用サーバに接続されてから一定時間経過後に前記メモリ内のデータを消去するタイマとを具備することを特徴とする。

## 【 0 0 1 4 】

請求項 7 に記載の発明は、請求項 1 ～請求項 3 のいずれかの項に記載のコンテンツレンタルシステムにおいて、前記記録媒体は、コンテンツが格納されるコンテンツ格納部と、前記コンテンツを読み出す制御アルゴリズムが記憶されるメモリと、記録媒体が前記レンタル用サーバに接続されてから一定時間経過後に前記メモリ内のデータを消去するタイマとを具備することを特徴とする。

請求項 8 に記載の発明は、請求項 6 または請求項 7 に記載のコンテンツレンタルシステム前記レンタル用サーバによって充電され、前記タイマへ電源を供給するコンデンサを設けたことを特徴とする。

## 【 0 0 1 5 】

請求項 9 に記載の発明は、顧客が所持する記憶媒体にコンテンツがダウンロードされ、前記顧客が所持する IC カード内のデータに基づいて前記コンテンツのセキュリティ管理が行われるコンテンツレンタルシステムにおいて、前記コンテ

ンツを製作するコンテンツ製作所と、前記コンテンツ製作所において作製されたコンテンツを複数の貸し出し事業者へ配信する管理センタと、前記貸し出し事業者が管理する店舗内に設けられたレンタル用サーバであって、前記管理センタから配信されたコンテンツが記録され、該記録されたコンテンツを前記顧客の指定に応じて前記記録媒体にダウンロードすると共に、前記ＩＣカード内のデータに基づいて前記コンテンツのセキュリティを管理するレンタル用サーバと、前記顧客の家に設けられ、前記記録媒体内のコンテンツを再生すると共に、前記ＩＣカード内のデータに基づいて前記コンテンツのセキュリティを管理する再生装置とからなることを特徴とするコンテンツレンタルシステムである。

## 【0016】

請求項１０に記載の発明は、請求項９に記載のコンテンツレンタルシステムにおいて、前記ＩＣカードが前記再生装置にセットされた時、前記再生装置がＩＣカードの認証を行い、前記ＩＣカードが前記再生装置の認証を行うことを特徴とする。

請求項１１に記載の発明は、請求項１０に記載のコンテンツレンタルシステムにおいて、前記再生装置の認証は、前記再生装置が再生装置公開鍵証明書を前記ＩＣカードへ送信し、前記ＩＣカードが該再生装置公開鍵証明書を認証する処理であり、前記ＩＣカードの認証は、前記ＩＣカードがＩＣカード公開鍵証明書を前記再生装置へ送信し、前記再生装置が該ＩＣカード公開鍵証明書を認証する処理であることを特徴とする。

## 【0017】

請求項１２に記載の発明は、前記再生装置の認証は、請求項１０に記載のコンテンツレンタルシステムにおいて、前記ＩＣカードが乱数を再生装置公開鍵によって暗号化して再生装置へ送信し、前記再生装置が前記暗号化された乱数を再生装置秘密鍵によって復号して前記ＩＣカードへ送信し、前記ＩＣカードがその復号化された乱数に基づいて認証することを特徴とする。

請求項１３に記載の発明は、請求項１０に記載のコンテンツレンタルシステムにおいて、前記ＩＣカードの認証は、前記再生装置が乱数をＩＣカード公開鍵によって暗号化してＩＣカードへ送信し、前記ＩＣカードが前記暗号化された乱数

をＩＣカード秘密鍵によって復号して前記再生装置へ送信し、前記再生装置がその復号化された乱数に基づいて認証することを特徴とする。

## 【 0 0 1 8 】

請求項 1 4 に記載の発明は、請求項 9 に記載のコンテンツレンタルシステムにおいて、前記ＩＣカードが前記レンタル用サーバにセットされた時、前記レンタル用サーバが前記管理センタと協働でＩＣカードの認証を行うことを特徴とする。

請求項 1 5 に記載の発明は、請求項 1 4 に記載のコンテンツレンタルシステムにおいて、前記ＩＣカードの認証は、前記ＩＣカードがＩＣカード公開鍵証明書を前記レンタル用サーバを介して前記管理センタへ送信し、前記管理センタが該ＩＣカード公開鍵証明書を認証する処理であることを特徴とする。

## 【 0 0 1 9 】

請求項 1 6 に記載の発明は、請求項 1 4 に記載のコンテンツレンタルシステムにおいて、前記ＩＣカードの認証は、前記管理センタが乱数をＩＣカード公開鍵によって暗号化して前記レンタル用サーバを介してＩＣカードへ送信し、前記ＩＣカードが前記暗号化された乱数をＩＣカード秘密鍵によって復号して前記レンタル用サーバを介して管理センタへ送信し、前記管理センタがその復号化された乱数に基づいて認証することを特徴とする。

請求項 1 7 に記載の発明は、請求項 1 4 に記載のコンテンツレンタルシステムにおいて、前記ＩＣカードが前記レンタル用サーバにセットされた時、前記ＩＣカードが再生装置公開鍵証明書を前記レンタル用サーバを介して前記管理センタへ送信し、前記管理センタが該再生装置公開鍵証明書に基づいて再生装置の認証を行うことを特徴とする。

## 【 0 0 2 0 】

請求項 1 8 に記載の発明は、請求項 9 に記載のコンテンツレンタルシステムにおいて、前記レンタル用サーバは、前記記憶媒体およびＩＣカードがセットされ、前記顧客がコンテンツを選択した時、契約内容を前記ＩＣカードへ送信し、前記ＩＣカードが前記契約内容を暗号化して前記レンタル用サーバを介して前記管理センタへ送信し、前記管理センタが前記契約内容を復号し認証した後前記顧客

が選択したコンテンツの暗号鍵を暗号化して前記レンタル用サーバを介して前記 I C カードへ送信し、前記 I C カードが前記コンテンツの暗号鍵を復号して認証した後、前記レンタル用サーバへ正常通知を行い、前記レンタル用サーバが前記正常通知を受け、コンテンツを前記記憶媒体にダウンロードすることを特徴とする。

#### 【 0 0 2 1 】

請求項 1 9 に記載の発明は、請求項 9 に記載のコンテンツレンタルシステムにおいて、前記再生装置は、前記記憶媒体および前記 I C カードがセットされた時、前記 I C カードへコンテンツ暗号鍵送信要求を行い、前記 I C カードが該送信要求を受け、コンテンツ暗号鍵を暗号化して前記再生装置へ送信し、前記再生装置が前記暗号化されたコンテンツ暗号鍵を復号し認証した後、復号したコンテンツ暗号鍵を用いて前記コンテンツを再生することを特徴とする。

#### 【 0 0 2 2 】

##### 【発明の実施の形態】

##### <第 1 実施形態>

図 1 は本発明の第 1 の実施形態によるコンテンツレンタルシステムの全体構成を示すブロック図である。この図において、映像製作会社 1 は、映像マスターを作成するもので、ハードウェアとしては脚本に沿った映像を撮影する撮影用カメラと、フィルムで起こされた場合にはデジタル画像に変換するデジタル画像変換処理装置と、それらの管理・制御用コンピュータ等が備えられている。

#### 【 0 0 2 3 】

ビデオソフトデuplicater（複製業者）2 は、映像製作会社 1 から供与された映像マスターから子マスター記録媒体を複製するための複製装置を備えている。また、映像マスターのタイトル名や、その主演者の俳優名、映像時間などの情報、何本の子マスター記録媒体を作製したか等の管理や、経営、運営上の数字的な管理を行っている。

#### 【 0 0 2 4 】

各種著作権協会 5 は、著作権に関する著作権者と契約した内容に従って、映像マスター或いは音楽、芸術等の著作権に応じた料金の徴収と、著作権侵害に対す

る管理と、徴収した料金を各著作権者へ分配する配分等の役割を実行しており、それぞれの役割に応じたサーバ端末により運営している。

## 【0025】

貸し出し事業者3は、ビデオソフトデuplicーター2から分配された子マスター記録媒体に基づいて顧客に貸し出す持ち運び可能な記録媒体（リムーバブル型磁気ディスク媒体；以下RHDDという）を製作するRHDD製作装置としてダウンロード専用のサーバ端末を備え、需要に応じてRHDDを製作し、希望する顧客に貸し出す。また、貸し出した時と引き取ったときの期間計算と、貸出料金を計算して、顧客から貸出料金の徴収を行うサービス業のためのサーバ端末を備え、さらに、ネットワークを介して協力関係のある他の貸し出し事業者との連絡や各種著作権協会やビデオソフトデuplicーター2との情報交換やその他情報の通信を行うネットワーク用端末装置を備えている。

顧客4は、一般貸し出し用のRHDDを数時間又は数日、貸し出し事業者3から貸し出しを受ける。

## 【0026】

次に、上記システムの動作を説明する。

まず、映像製作会社1は、映像マスターを製作して映画館や音楽会等に供給する一方、レンタル用に分配する用意をする。次に、ビデオソフトデuplicーター2と、ビデオソフトの頒布権行使委託契約11を締結する。ビデオソフトデuplicーター2は映像製作会社1から、磁気ディスク装置に直接記録可能なデジタルマスターテープの有償配布13を受け、使用料金の支払い12を行う。また、貸し出し情報および返却情報データ14を共有する意味で、映像製作会社1と、映像マスターの映像タイトル名、子マスター記録媒体の作製本数、返却期日などの情報を通知し合う。

## 【0027】

また、ビデオソフトデuplicーター2は各種著作権協会5との関係では、著作権に関する映像マスター及び子マスター磁気ディスク媒体のタイトル名と複製の本数等の情報通知義務を使用料徴収委託契約51によって契約し、また実績から計算した著作権料金支払い52を行う。



## 【0028】

また、ビデオソフトデuplicーター2と貸し出し事業者3の間では、上記子マスター記録媒体等に関わる供与保守契約21が締結される。ビデオソフトデuplicーター2では貸し出し事業者3向けに、デジタルマスターテープをもとに子マスター記録媒体として映像情報を記録した子マスター磁気ディスク媒体とその貸し出し備品の供給22を、物理的な手段、具体的には宅配便などにより貸し出し貸し出し、事業者3に配布される。貸し出し事業者3からビデオソフトデuplicーター2へ子マスター磁気ディスク媒体の使用料金支払い23を行い、貸し出し情報および返却情報データ24を通知する。

## 【0029】

また、デジタルマスターテープの映像情報を、衛星放送もしくはインターネットを介して、複数の貸し出し事業者3に同時に配信され、貸し出し事業者3で直接、子マスター磁気ディスク装置が作成される場合もある。

## 【0030】

また、貸し出し事業者3と顧客4の間では、まず相互にレンタル料金、レンタル期間、レンタル料金等のレンタル契約31を行い、RHDDの貸し出し32を行い、顧客4から貸し出し事業者3へレンタル料金支払い33が現金或いはクレジットで行われる。

## 【0031】

また、広告契約をビデオソフトデuplicーター2と締結したスポンサーが希望するCM映像を、映像製作会社1の同意のもとで、映像ビデオソフトの放映が開始する前か、終了した後に挿入した子マスター磁気ディスク装置をビデオソフトデuplicーター2で作成するか、もしくはCM映像のみを記録した子マスター磁気ディスク装置をビデオソフトデuplicーター2で作成する。一方、映像ビデオソフト情報と同様に、CM情報を衛星放送もしくはインターネットを介して、複数の貸し出し事業者3に同時に配信し、貸し出し事業者3でCM付きの子マスター磁気ディスク装置が作成される場合もある。

## 【0032】

貸し出し事業者3において、例えば、レンタル用映像磁気テープが貸し出し用

として準備されていることを確認した顧客は、顧客の希望により、映像ビデオソフトとCM情報が記録されたRHDDの貸し出しを受けることができる。この際に、貸し出し事業者3では、映像ビデオソフトを記録した子マスター磁気ディスク装置とCM情報を記録した子マスター磁気ディスク装置をもとに、それらの情報を記録したRHDDが作成されるが、このダウンロード処理は、貸し出し事業者3に設置された専用サーバ端末を用いて行われる。

## 【0033】

RHDDを貸し出す際に、顧客4と貸し出し事業者3との間で結んだレンタル契約に基づいたレンタル料金を、貸し出し事業者3は顧客4から徴収する。また、この貸し出しの際に、RHDDに記録した映像タイトル名、貸し出し期間、貸し出した顧客名、顧客管理用の顧客の属性データを印刷した貸し出しおよび顧客管理用ラベルが、専用サーバ端末と一体となったラベルメーカー装置により作成される。作成したラベルを貼り付けたRHDDが顧客に貸し出される。この際、ラベルリーダーを備えたPOS端末で映像タイトル名、貸し出し期間、貸し出した顧客名、顧客管理用の顧客の属性データが、上記一連の商行為に関係する各種著作権協会5、映像製作会社1、ビデオソフトデュプリケーター2、貸し出し事業者3間で共有し、各者の間で交わされる使用料金請求の根拠を確認するためのデータとして用いられる。

## 【0034】

また、顧客がRHDDを返却した際に、その貸し出しおよび顧客管理用ラベルの読み取りを行い、返却の確証とされる。このラベル処理による使用料金請求の他に、各種著作権協会5、映像製作会社1、ビデオソフトデュプリケーター2、貸し出し事業者3が所有するサーバ端末がインターネットを介して結合しており、ビデオソフトデュプリケーター2で映像マスターから作成された映像タイトル名、それぞれの映像デジタルマスターテープから作成した子マスター磁気ディスク媒体の本数、子マスター磁気ディスク媒体を配布した貸し出し事業者名、貸し出し事業者3で子マスター磁気ディスク媒体から顧客貸し出し用に作成した映像タイトル、RHDDの貸し出し本数、貸し出し期間、貸し出しを受けた顧客4の属性、および顧客4から貸し出し事業者3への返却に関する情報を共有すること

ができ、この共有したデータに基づいて著作権料、上記の商行為に対して相互に合意のうえで予め定められた料金の請求、徴収が行われる。

## 【0035】

上記一連の商行為を正確かつ効率よく行うためには、ビデオソフトデュプリケーター2と貸し出し事業者3間で一連の商行為に関わる各種経営データ情報と、ダウンロード処理等の技術的な行為を行うサーバ端末の一元的な保守管理は必須である。このため、貸し出し事業者3に設置されたダウンロード用のサーバ端末装置、ダウンロード用サーバ端末装置と連動して貸し出し用ラベルを作成するラベルメーカー、子マスター磁気ディスク媒体の駆動装置、および貸し出し用のRHDDの記録媒体の保守管理に関わる業務委託契約をビデオソフトデュプリケーター2と貸し出し事業者3との間で締結し、委託契約に関わるすべての機器や記録媒体の配送、保守、管理の業務に関わる費用を、貸し出し事業者3からビデオソフトデュプリケーター2がインターネットを介して相互に得られる情報に基づいて徴収するシステムが構築されている。

## 【0036】

不正なコピー行為によるデジタル映像情報の流出を防止するために、子マスター記憶媒体とRHDD自身にクロック機能を設け、ビデオソフトデュプリケーター2／貸し出し事業者3間および貸し出し事業者3／顧客4間で契約した一定時間経過後または所定のダウンロード回数に達した時点で、それぞれの記録媒体から自動的に映像情報が消去されるような機能をRHDDを装着した駆動装置に持たせることも可能である。

## 【0037】

次に、上記実施形態の変形例について、図2に基づいて説明する。始めに、ビデオソフトデュプリケーター2とCMの広告スポンサー9が広告契約を交わし、ビデオソフトデュプリケーター2はCMスポンサー9が著作権を有するCMのデジタルマスターテープの配布を受ける。その配布に対応して広告スポンサー9はビデオソフトデュプリケーター2に広告料金を支払う。ビデオソフトデュプリケーター2は、このCM情報をビデオソフト情報の前後に記録した子マスター磁気ディスク媒体か、CM情報のみを記録した子マスター磁気ディスク媒体を作成し

、貸し出し事業者3に配布するか、ビデオソフトと同様に衛星放送またはインターネットを介して貸し出し事業者3に配信する。貸し出し事業者3は、これらの子マスター磁気ディスク媒体をもとにビデオソフトとCM情報が記録されたRHDDを作成し、顧客4に貸し出す。

## 【0038】

ビデオソフトデュプリケーター2はCMスポンサー9の有するCM情報が記録されたRHDDの貸し出しデータをインターネット等の通信ネットワークを介して各貸し出し事業者3から収集し、その結果に基づいてCMスポンサー9からCM料金として広告料金を徴収する。また、ビデオソフトデュプリケーター2は、貸し出し事業者3と交わした契約に基づいて、CM料金の一部を貸し出し事業者3に支払う。また、CM映像内にCMスポンサー9が提供するホームページ、プレゼント、宝くじなど、顧客4が利益を受けることができる情報画面に移行するアイコンを設け、顧客4がCM映像視聴中にアイコンをクリックすると、インターネットを介して上記情報画面に移行する。

## 【0039】

顧客4は、貸し出し事業者3からレンタルしたRHDD17をRHDD再生装置18に装着して、テレビやモニター等のテレビ画面19に表示し、アイコン1、2、3が表示されるので、キーボード或いはマウス等の操作盤によってアイコンをクリックすることで、顧客4の好みの情報を選択する。このアイコンの選択は、テレビをモデムを介してネットワーク回線に接続し、さらにインターネットを介して、CMサーバ10に接続する。これにより、CMサーバ10のWebページがテレビに表示され、選択されたアイコンに応じた広告、プレゼント、宝くじ等が表示される。

## 【0040】

ビデオソフトデュプリケーター2は、サーバ10からインターネットを介して、選択されたアイコンに応じた情報、すなわち、CM視聴顧客数、顧客属性情報等のデータを受け取る。そして、受け取ったデータに基づいて顧客4の属性およびCM視聴顧客数をCMスポンサー9に提示することによって、CM料金をCMスポンサー4から徴収し、その徴収料金をビデオソフトデュプリケーター2と貸

し出し事業者3との間で交わした契約に基づいて、両者で配分する。

【0041】

この場合の広告料金は、CMに対する実績数に応じて支払われるので、広告スポンサー9にとっても広告効率は高くなり、予測した数に応じて支払う広告料金よりも、その広告に対応する販売数との関係は別として、広告の伝送達成率は明確となる。

【0042】

なお、上記実施形態では、レンタル種類として映像情報について説明したが、音声（音楽）情報であってもよく、さらに、辞書や美術情報等、或いはパソコン用のソフトウェア等の多彩なマルチメディアを提供することも可能である。

【0043】

<第2実施形態>

次に、上述した各実施形態におけるRHDD17、貸し出し事業者が管理するダウンロード用サーバおよび顧客が自宅において使用する再生装置について詳述する。

図3は、RHDD17の構成を示すブロック図である。この図において、コンテンツ格納部101は、制御部102により読み書き制御され、貸し出し事業者が管理するダウンロード用サーバ106から受け取ったコンテンツが格納される部分で、磁気ディスクや不揮発性メモリなどが用いられる。

【0044】

制御部102は、サーバ106から電力供給を受けたときにコンテンツ格納部101、揮発性メモリ104を読み書き制御する。また、制御部102は、RHDD17に接続された機器が正規のものであるかどうかを確認する機能を持つ。外部インタフェース103は、RHDD17をサーバ106または再生装置と接続するインタフェースであり、サーバ106または再生装置から電力の供給を受け、コンテンツと、コンテンツの再生に必要な情報とを外部入力または外部出力する。また、サーバ106との接続が確認されたとき、サーバ106の電力によってコンデンサ105を充電する。揮発性メモリ104は、コンデンサ105でバックアップされており、制御部102により読み書き制御され、暗号復号鍵が

記憶される。

【0045】

次に、上記RHDD17の動作を図4に示す示すフローチャートにしたがって説明する。

まず、サーバ106には、暗号化されたコンテンツとそのコンテンツの暗号を復号するための暗号復号鍵とが格納されている。このサーバ106とRHDD17は外部インタフェース103を介して接続される（ステップS1）。このとき、RHDD17は、接続された機器が正規のサーバであるかをチェックする（ステップS2）。チェックの方法としては、外部インタフェース103の外形が合っていれば良しとする最も簡単なチェック方法から、制御部102がRHDDとサーバとの間で認証を行うチェック方法まで様々な方法がある。これら外部インタフェース103または制御部102の確認部のチェックにより、接続されたサーバが正規のサーバでないと判断されると、充電は行われず終了する。

【0046】

外部インタフェース103または制御部102の確認部のチェックにより、サーバ106が正規のサーバであることが確認されると、サーバの電力が外部インタフェース103を通じてコンデンサ105に供給され、充電が行われる（ステップS3）。このとき、外部インタフェース103の外形チェックのみで確認する場合、接続された途端にサーバの電力が外部インタフェース103を通じてコンデンサ105に供給され、充電が行われる。その他の場合、制御部102が外部インタフェース103に対してコンデンサ105へ電力を供給するよう指示を出し、充電が行われる。

【0047】

続いて、制御部102は、外部インタフェース103を通じて暗号化されたコンテンツをサーバ106から受け取り、コンテンツ格納部101に格納する（ステップS4）。同様に、制御部102は外部インタフェース103を通じてコンテンツの再生に必要な暗号復号鍵をサーバ106から受け取り、揮発性メモリ104に格納する（ステップS5）。

サーバ106によってコンテンツが書き込まれたRHDD17は、ユーザの

持つ再生装置に接続されてコンテンツが再生される。

【0048】

図5は、RHDD17が再生装置109に接続された時の構成を示すブロック図であり、図6はこの場合の動作を示すフローチャートである。

まず、RHDD17を再生装置に接続する（ステップS11）。この接続が行われると、RHDD17は、接続された装置が正規の再生装置かどうかをチェックする（ステップS12）。チェックの方法はサーバ106をチェックしたのと同様な方法を用いることができる。正規の再生装置であることが確認されると、制御部102は揮発性メモリ104に格納されていた暗号復号鍵を読み出し、外部インタフェース103を通じて暗号復号部107に渡す（ステップS13）。次に、制御部102はコンテンツ格納部101から暗号化されたコンテンツを読み出し、外部インタフェース103を通じて暗号復号部107に送る（ステップS14）。再生装置側では、暗号復号部107が暗号化されたコンテンツを復号した後、再生部（ディスプレイ装置）108で再生する（ステップS15）。

【0049】

本実施形態のRHDD17は、接続された相手が正規のサーバでない場合、外部インタフェース103からコンデンサ105への電力供給を行わない。これにより、ユーザの手元にあるRHDD17のコンデンサ105に貯えられた電力は減りつづけ、ある期間が経つと揮発性メモリ104に格納されたデータをバックアップできる電圧を下回る。そうになると、揮発性メモリ104に格納された暗号復号鍵が失われる。コンテンツ格納部101には暗号化されたコンテンツが格納されているが、それを復号するための暗号復号鍵が失われてしまうため、再生装置109に接続してもコンテンツを再生することができない。このようにして、ある期間が経過するとコンテンツの再生が不可能になる。なお、ある期間とは、コンデンサの容量と揮発性メモリ104をバックアップする時に流れる電流の量によって決まり、コンデンサ105の容量に選ぶことで、ある程度消えるまでの期間を制御することができる。

【0050】

上記の動作説明では、サーバ106から暗号化されたコンテンツと暗号復号鍵

の2つをRHDD17に格納するとしたが、一旦、暗号化されたコンテンツが格納されれば、後で、暗号復号鍵だけをサーバ106から受け取って揮発性メモリ104に格納してもよい。また、説明上、制御部102と揮発性メモリ104とを別のブロックにしたが、制御部102の内部に揮発性メモリ104を持たせることも考えられる。こうすることにより、制御部102と揮発性メモリ104間のバスを外部に出さずにすみ、揮発性メモリのデータをコピーされることが起きにくくなる。

#### 【0051】

上記RHDD17は、上述した暗号復号鍵に代えて、制御部102のコンテンツ読み出し制御用の制御データを用いることもできる。この場合の動作について、次に説明する。この場合、構成は同じであるので図3を参照する。

制御部102の動作は、コンテンツ格納部101から読み出す動作と、それ以外の動作とに大きく分けることができる。このうち、コンテンツ格納部101から読み出す動作以外の動作に関わる制御アルゴリズムを不揮発性メモリ104に格納しておく。

#### 【0052】

RHDD17は、サーバ106と接続されると、まず、サーバ106が正規のサーバかどうかをチェックする。正規のサーバであることが確認されると、外部インタフェース103を通じてコンデンサ105を充電する。その後、コンテンツ格納部101からコンテンツを読み出すための読み出し制御アルゴリズムをサーバ106から受け取り、揮発性メモリ104に格納する。

#### 【0053】

制御部102は、コンテンツ格納部101からの読み出しが必要になったら揮発性メモリ104の制御アルゴリズムを参照し、コンテンツ格納部101からコンテンツを読み出す。しかしながら、再度サーバに接続しないかぎりコンデンサ105に貯えられた電力が減りつづけ、ある期間が経つと揮発性メモリ104に格納された読み出し制御アルゴリズムが消えてしまう。コンテンツ格納部101にはコンテンツが格納されているが、それを読み出すための読み出し制御アルゴリズムが失われてしまうため、再生装置に接続してもコンテンツを再生すること



ができない。このようにして、ある期間が経過するとコンテンツの再生が不可能になる。

【0054】

コンテンツの再生に上述した制御アルゴリズムを用いる場合、コンテンツ格納部101に格納されるコンテンツは、暗号化されていなくてもよい。この場合、RHDD17の中にMPEG (Moving Picture Experts Group) デコーダ部を内蔵させ、コンテンツデータそのものが外部に流れないようにすることで、暗号化されていないコンテンツデータが外部に流れるのを防ぐことができる。なお、コンテンツの再生に必要な情報としては、読み出し制御アルゴリズム以外にも、ディスクのフォーマットパラメータなどの読み出し制御パラメータも利用することができる。

【0055】

図7は、RHDDの第2の構成例を示すブロック図、図8はその動作を示すフローチャートである。これらの図において、サーバ106には、コンテンツのレンタル時間情報が格納されている。このサーバ106とRHDD17aは外部インタフェース103で接続される(ステップS21)。このとき、RHDD17aは、接続された機器が正規のサーバであるかをチェックする(ステップS22)。チェックの詳細に付いては、既に説明してあるので省略する。

【0056】

正規のサーバであることが確認されると、制御部102は、外部インタフェース103を通じて、サーバ106からレンタル時間情報を受け取る(ステップS23)。レンタル時間情報は、例えば、2日間や48時間などの時間でもよいし、1728000などのタイマのカウント値でもよい。時間情報で受け取った場合は、制御部102にてタイマ109にセットする値に換算する。そして、換算された値をタイマ109に書き込む(ステップS24)。さらに、制御部102は、外部インタフェース103を通じて、サーバ106からコンテンツとコンテンツの再生に必要な暗号復号鍵とを受け取り、コンテンツをコンテンツ格納部101に格納し、暗号復号鍵を揮発性メモリ104に格納する(ステップS25)。その後、制御部102は、タイマ109に指示してカウントダウンを開始させ

る（ステップS26）。

【0057】

タイマ109が動作を始めると、内部のカウンタが0になるかチェックする（ステップS27）。カウンタが0になると、タイマ109は、不揮発性メモリ104に指示を出し、不揮発性メモリ104に格納された暗号復号鍵を消去する（ステップS28）。消去方法としては、タイマの109の内部に揮発性メモリ104の一定領域に0を書き込む回路を設けてもよいし、電池110から揮発性メモリ104に供給している電源ライン上に設けたスイッチを切断するような機構を設けることも可能である。

【0058】

上記の動作説明上、制御部102、揮発性メモリ104、タイマ109を別々のブロックにしたが、制御部102の内部に揮発性メモリ104とタイマ109を持たせることも考えられる。こうすることにより、タイマ109から揮発性メモリ104へ出される消去指示を改変される恐れが少なくなり、消去動作がより確実になる。

【0059】

図9は、RHDDの第3の構成例を示すブロック図である。この図に示すRHDD17bは、図7のRHDD17aにおける電池110をコンデンサ105で代用し、揮発性メモリ104、タイマ109をバックアップする。コンデンサ105が制御部102の許可に基づき外部インタフェース103を通してサーバから電力の供給を受けること以外は、図7のRHDD17aと同様である。

【0060】

この構成例では、通常、タイマ105に設定する時間よりも長い時間バックアップ可能なようにコンデンサ105の容量を選択する。これにより、タイマ105に間違って長い値を設定した場合でも、電池110でバックアップされるよりも短い時間でコンテンツが再生できなくなるため、いつまでもコンテンツが再生できるという事故が起きにくい。

【0061】

以上説明してきたRHDDの説明では、コンテンツ格納部101を不揮発性の

媒体として説明してきたが、このコンテンツ格納部 1 0 1 を揮発性メモリで構成し、電池やコンデンサでバックアップする変形例も可能である。たとえば、図 1 0 は、RHDD の第 4 の構成例を示すブロック図である。図 1 0 を参照すると、この変形例の RHDD 1 7 c は、コンテンツ格納部 1 0 1 に揮発性メモリを使用し、コンデンサ 1 0 5 が、コンテンツ格納部 1 0 1 の電力もバックアップしている。このため、コンデンサ 1 0 5 の電荷が無くなると、揮発性メモリ 1 0 4 に格納された暗号復号鍵が消えるだけでなく、コンテンツそのものも消えるので、適切な充電が行われなければ、所定の時間が経過するとコンテンツの再生が不可能となる。なお、説明上、コンテンツ格納部 1 0 1 と揮発性メモリ 1 0 4 を分けて記述したが、これらコンテンツ格納部 1 0 1、揮発性メモリ 1 0 4 は、同じデバイスであってもよい。

## 【 0 0 6 2 】

図 1 1 は、RHDD の第 5 の構成例を示すブロック図、図 1 2 および図 1 3 はその動作を示すフローチャートである。

まず、サーバと RHDD 1 7 d とが外部インタフェース 1 0 3 を介して接続される（ステップ S 2 9）。このとき、RHDD 1 7 d は、接続された機器が正規のサーバであるかをチェックする（ステップ S 3 0）。チェックの方法については、既に説明した方法と同様なので、ここでは省略する。

## 【 0 0 6 3 】

チェックによりサーバが正規のサーバであることが確認されると、制御部 1 0 2 は、外部インタフェース 1 0 3 を通じて暗号化されたコンテンツをサーバから受け取り、データ格納部 1 1 5 に格納する（ステップ S 3 1）。同様に、制御部 1 0 2 は外部インタフェース 1 0 3 を通じて暗号復号鍵をサーバから受け取り、データ格納部 1 1 5 に格納する（ステップ S 3 2）。その後、制御部 1 0 2 はコンテンツが読めなくなるまでの有効期限となる時間情報をサーバから受け取り、有効期限をタイマ 1 1 9 にセットし、カウントを開始させる（ステップ S 3 3）。なお、ステップ S 3 1 ～ S 3 3 の順序はどのような順序でも構わない。

## 【 0 0 6 4 】

一旦、サーバから有効期限情報を受け取ってタイマ 1 1 9 に書き込みタイマ 1

09が動作を開始すると、タイマ119は電池110でバックアップされているため、サーバから切り離されてもカウントを続ける。タイマ119がカウントダウン型であればカウントが0になったとき、あるいは、カウントアップ型であればカウントが有効期限を示す値になったとき、タイマは動作を停止し、有効期限が来たことを保持する。

#### 【0065】

図13は、RHDD17dがユーザの持つ再生装置に接続されたときの最初の動作を示すフローチャートである。まず、RHDD17dを再生装置に接続する（ステップS34）。このとき、RHDD17は再生装置から主電源の供給を受ける。続いて、RHDD17d内の制御部102は、タイマ119の値が有効期限を過ぎているかどうかをチェックする（ステップS35）。もし過ぎていれば、制御部102は、データ格納部115に格納された暗号復号鍵を消去する。もし過ぎていなければ、そのまま終了し、コンテンツ再生動作に移る。コンテンツ再生動作については、既に説明した動作（ステップS11～S15）と同じなので、ここでは省略する。

#### 【0066】

なお、上記の説明では、タイマ119をバックアップする電源として電池110を用いたが、コンデンサを用いることも可能である。コンデンサへの充電はサーバや再生装置から行われる。

このようにして、有効期限が過ぎた場合、外部から主電源が供給されるとすぐにデータ格納部に格納された暗号復号鍵を消去するので、有効期限が過ぎると暗号復号鍵を不正に取り出すことができなくなる。

#### 【0067】

以上説明してきたRHDDにおいては、制御部102がコンテンツ格納部101またはデータ格納部115の読み書き制御を行うとしていたが、コンテンツ格納部101またはデータ格納部115の読み書き制御を正規のサーバや再生装置側の媒体読み書き部で行い、媒体読み書き部を持たないRHDDとする変形例も可能である。例えば、図14は、RHDDの第6の構成例を示すブロック図であり、コンテンツ格納部101は、制御部102から独立しており、媒体読み書き

部を持たない。逆に、サーバ121が、媒体読み書き部111を持ち、コンテンツ格納部101の読み書き制御を行う。

#### 【0068】

このRHDD17eにおいて、コンテンツとコンテンツの再生に必要な情報は、サーバ121のコンテンツ情報格納部113に格納されており、サーバ側制御部112は、サーバ側コンテンツ情報格納部113からコンテンツを読み出し、媒体読み書き部111を通してのコンテンツ格納部101に書き込む。一方、暗号復号鍵は、サーバ側制御部112がサーバ側コンテンツ情報格納部113から読み出し、RHDD17eの外部インタフェース103を通して制御部102に渡す。制御部102ではそれを揮発性メモリ104に格納する。コンデンサ105の充電の仕組みについては、今まで説明してきたことと同様なので省略する。

#### 【0069】

図15は、再生装置の他の構成例を示すブロック図である。再生装置122の制御部114は、読み出し制限機能付き媒体の揮発性メモリ104に格納された暗号復号鍵を制御部102、外部インタフェース103を通して受け取り、暗号復号部107に送る。なお、揮発性メモリ104内に媒体読み書き部111の制御データが記憶されていた場合は、再生装置側制御部114がそのデータを媒体読み書き部111に送る。その後、再生装置122はコンテンツ再生制限機構付き媒体のコンテンツ格納部101からコンテンツを読み出し、暗号復号部107で復号した後、再生部108で再生する。しかし、コンデンサ105によりバックアップされる期間が過ぎていれば、たとえ、偽の媒体がコンテンツをコピーして格納していても、暗号復号鍵が消えているため、コンテンツを再生できない。

#### 【0070】

上述したRHDD17～17eによれば、ある期間が経過するとコンテンツの再生に必要な情報が消えてしまうため、コンテンツの再生が不可能になる。従って、レンタルシステムに適用した場合、コンテンツ媒体を返却しなくてもよいレンタルシステムの構築が可能となる。また、タイマを備えた場合、コンテンツの再生に必要な情報が消えるまでの期間を正確に設定することができる。

#### 【0071】

また、正規のサーバと確認したときにコンデンサを充電するので、偽のサーバによりコンテンツの再生に必要な情報が消えるまでの期間を不正に延長することを防ぐことができる。また、コンテンツが一旦格納された場合、手渡し時、コンテンツの再生に必要な情報のみサーバから受け取ればよいので、作業時間が大幅に減る。また、コンテンツの再生に必要な情報として媒体読み書き制御データを用いると、ある期間の経過後にデータが失われるとコンテンツを読み出すこともできなくなるため、不正に読み出される危険性が大幅に減る。また、内部の電池（あるいはコンデンサ）でバックアップするのはタイマだけとし、有効期限が過ぎた場合、外部から主電源が供給されると直ぐに、データ格納部に格納された暗号復号鍵を消去することもでき、内部の電池やコンデンサの容量を小さくでき、コストを削減できる。

## 【 0 0 7 2 】

また、媒体読み書き部をサーバや再生装置側に持たせ、コンテンツ再生制限機構付き媒体の構成を簡略化することもでき、コストを大幅に削減することが可能となる。また、再生装置の媒体読み書き部の制御データをコンテンツ再生制限機構付き媒体から受け取ることができるため、正規のコンテンツ再生制限機構付き媒体以外ではコンテンツを読み出すこともできず、コンテンツを不正に再生される危険性を大幅に減らすことができる。

## 【 0 0 7 3 】

## &lt;第3実施形態&gt;

次に、RHDDの構成をコンテンツを記録する記録媒体のみとし、さらに、ICカードおよび公開鍵／秘密鍵を使用してコンテンツのセキュリティを厳密に確保した実施形態を説明する。

図16は同実施形態の構成を示すブロック図である。この実施形態においては、複数の貸し出し事業者3を管理する管理センタ160を設けており、この管理センタ160が複数の貸し出し事業者3のダウンロード用サーバ162とネットワーク164を介して接続されている。そして、この管理センタ160が図1におけるビデオソフトデュプリケータ2に相当する。また、サーバ162にコンテンツ記録媒体166およびICカード167が接続される。また、170はユ

ーザ宅に設けられた再生装置であり、この再生装置170にコンテンツ記録媒体166およびICカード167が接続されて、コンテンツ記録媒体166内のコンテンツが再生される。

【0074】

管理センタ160はコンテンツ毎に暗号化したコンテンツ暗号鍵と、全ICカードの公開鍵証明書と、全再生装置の公開鍵証明書と全ICカードと全再生装置のペア情報を保管しており、サーバ162を介してICカード167からICカードの公開鍵証明書と再生装置の公開鍵証明書を受信し正当性を確認することができる。

またサーバ162を介してICカード167と相互認証した後、サーバ162からの所定の手続きによりコンテンツ暗号鍵とレンタル期間情報をICカード167へ配信することができる。サーバ162は管理センタ160で保管しているコンテンツ鍵で暗号化されたコンテンツが記録されており、ユーザはサーバ162によってコンテンツをレンタル購入するための操作を行うことができる。サーバ162は管理センタ160とICカード167との所定の手続きにより、コンテンツ記録媒体166に暗号化されたコンテンツをダウンロードすることができる。

【0075】

ICカード167はサーバ162を介して、コンテンツを暗号化したコンテンツ暗号鍵とレンタル期限情報をダウンロードし、レンタル期間中コンテンツ鍵を保管し、レンタル期間を過ぎるとコンテンツ鍵を消去することができる。また、ICカードはユーザが所有している再生装置170を相互認証し、所定の手続きによりレンタル期間中はコンテンツ鍵を配信することができる。コンテンツ記録媒体166は、管理センタ160とICカード167の所定の手続きによりサーバ162に記録されたコンテンツを記録することができる。また、コンテンツ記録媒体166はユーザが所有する再生装置170へ所定の手続き後、再生装置170の制御によりコンテンツデータが読み出される。

【0076】

ユーザが所有している再生装置170は、ICカード167との認証処理後の

所定の手続きにより IC カード 1 6 7 から送信されたコンテンツ鍵をレンタル期間中まで保管し、レンタル期間が過ぎるかあるいは電源が切断されるまで保持することができる。また、再生装置 1 7 0 はコンテンツ記憶媒体 1 6 6 から所定の手続きにより暗号化されたコンテンツを読み出し、IC カード 1 6 7 から読み出したコンテンツ暗号鍵によって暗号化されたコンテンツデータを復号し、レンタル期間中はコンテンツを再生することができる。

## 【 0 0 7 7 】

次に、図 1 6 に示す装置の動作を順を追って説明する。

まず、IC カード 1 6 7 は前もって再生装置 1 7 0 と接続し、IC カード 1 6 7 と再生装置 1 7 0 の相互認証を行う。IC カード 1 6 7 は正常であれば再生装置公開鍵の証明書を記憶する。次にユーザは IC カード 1 6 7 とコンテンツ記録媒体 1 6 6 を店舗へ持参しサーバ 1 6 2 に接続する。サーバ 1 6 2 は IC カード 1 6 7 が接続されると IC カード 1 6 7 から IC カード 1 6 7 の公開鍵証明書を読み出し、管理センタ 1 6 0 へ読み出した IC カード 1 6 7 の公開鍵証明書と共に相互認証の要求を行う。

## 【 0 0 7 8 】

管理センタ 1 6 0 は IC カード 1 6 7 の公開鍵証明書の有効性を確認し、IC カード 1 6 7 と相互認証を行う。次にサーバ 1 6 2 は再生装置 1 7 0 の公開鍵証明書を読み出し、管理センタ 1 6 0 へ読み出した再生装置 1 7 0 の公開鍵証明書を転送する。管理センタ 1 6 0 は再生装置 1 7 0 の公開鍵証明書の有効性を確認する。次にユーザはサーバ 1 6 2 へレンタルするコンテンツのタイトルとレンタル期間を入力すると、サーバ 1 6 2 は IC カードへコンテンツのタイトルとレンタル期間を含む再生情報を送信し、IC カード 1 6 7 から再生情報と再生情報の署名を読み出す。サーバ 1 6 2 は管理センタ 1 6 0 に対してコンテンツ暗号鍵を要求するデータとして再生情報と再生情報の署名データを送信する。

## 【 0 0 7 9 】

次に管理センタ 1 6 0 は、サーバ 1 6 2 からの再生情報と署名を検証してデータの正当性が確認された場合、コンテンツタイトルに対応するコンテンツ暗号鍵を再生装置の公開鍵を用いて暗号化し、署名データを IC カード 1 6 7 へサーバ



162を介して送信する。ICカード167はコンテンツ暗号鍵と署名データを検証し、正当性が確認された場合コンテンツ鍵をレンタル期間中のみ保管する。

【0080】

次にサーバ162は所定の手順により暗号化コンテンツをコンテンツ記録媒体166に転送し、ユーザは店舗にレンタル料金を支払い後、ICカード167とコンテンツ記録媒体166を受け取る。次にユーザは所有の再生装置170へICカード167とコンテンツ記録媒体166を接続する。再生装置170はICカード167と相互認証し、正当性が確認できるとICカード167からコンテンツ暗号鍵とレンタル情報と署名データを読み取ることができる。

【0081】

再生装置170はコンテンツ鍵、レンタル情報と署名データを照合しデータの正当性が確認されると、コンテンツ鍵をレンタル期間あるいは電源が切断されるまで保管する。再生装置170はコンテンツ記憶媒体166から暗号化されたコンテンツを読み出し、コンテンツ鍵で復号しレンタル期間中あるいは電源が切断されるまでコンテンツを再生する。

【0082】

図17を参照すると、管理センタ160の詳細な構成例が示されている。管理センタ160は制御部201、復号部202、暗号部203、圧縮部204、乱数発生部205、認証部206、通信部207、管理センタ秘密鍵記憶部208、管理センタ公開鍵記憶部209、コンテンツ鍵記憶部210、公開鍵データベース211、課金情報データベース212から構成される。管理センタ秘密鍵記憶部208には管理センタ160のみが所有する秘密鍵が記録されている。管理センタ公開鍵記憶部209には管理センタ秘密鍵と所定の方法によりペアとなる管理センタ公開鍵が記録されている。コンテンツ鍵記憶部210には、コンテンツ毎に暗号化した共通鍵が記憶されている。公開鍵データベース211には、全ICカードと全再生装置の公開鍵証明書と全ICカードと全再生装置のペア情報が記録されている。課金データベース212には、ユーザがレンタルしたコンテンツに関してのタイトルとレンタル期間とレンタル料金が記録されている。

【0083】

復号部202は通信部207を介して店舗のサーバ162からの暗号化データを受信すると制御部160の制御により、管理センタ秘密鍵記憶部208に記憶されている管理センタ秘密鍵、あるいは公開鍵データベース210に記録されたICカードの公開鍵や再生装置の公開鍵を使って暗号データを復号することができる。暗号部203は、通信部207を介して店舗のサーバ162へデータを送信する時、制御部201の制御で管理センタ秘密鍵記憶部208に記憶している管理センタ秘密鍵あるいは公開鍵データベースに記録されたICカードの公開鍵や再生装置の公開鍵を使いデータを暗号化することができる。圧縮部204はハッシュ関数を用いて制御部の制御により任意のデータの圧縮を行うことができる。乱数発生部205は制御部の制御により乱数を発生することができる。認証部206は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行うことができる。

## 【0084】

図18は、図16に示すサーバ162の詳細な構成を示すブロック図である。サーバ162は、制御部301、通信部302、ICカード入出力部303、コンテンツ記録媒体入出力部304、入力部305、表示部306、コンテンツ記憶部307から構成されている。通信部302は制御部の制御によりインターネット等のネットワーク164を介して管理センタ160と通信を行うことができる。ICカード入出力部303は制御部160の制御によりICカード167と通信することができる。コンテンツ記録媒体入出力部304は制御部160の制御によりコンテンツ記録媒体166へコンテンツ記憶部のコンテンツデータを出力することができる。入力部305はレンタルするコンテンツの選択とレンタル期間をユーザが操作し入力することができるユーザインターフェースである。表示部306はレンタルするコンテンツのタイトル表示とレンタル期間を表示するユーザインターフェースである。コンテンツ記憶部307は、暗号化されたコンテンツが記憶されている。

## 【0085】

図19は、図16に示すICカード167の詳細な構成を示す図である。

ICカードは制御部401、入出力部402、復号部403、暗号部404、

圧縮部 4 0 5、乱数発生部 4 0 6、認証部 4 0 7、ＩＣカード秘密記憶部 4 0 8、管理センタ公開鍵記憶部 4 0 9、ＩＣカード公開鍵証明書記憶部 4 1 0、再生装置公開鍵証明書記憶部 4 1 1、コンテンツ暗号鍵記憶部 4 1 2、タイマ 4 1 3、電池 4 1 4 から構成される。

#### 【 0 0 8 6 】

ＩＣカード秘密鍵記憶部 4 0 8 には、秘密鍵が記憶されている。管理センタ公開鍵記憶部 4 0 9 は、管理センタ公開鍵が記憶されている。ＩＣカード公開鍵証明書記憶部 4 1 0 は、管理センタ 1 6 0 が発行したＩＣカード公開鍵証明書が記憶される。再生装置公開鍵証明書記憶部 4 1 1 には、再生装置 1 7 0 から読み出される管理センタ 1 6 0 が発行した再生装置公開鍵証明書が記憶される。コンテンツ暗号鍵記憶部 4 1 2 は電池 4 1 4 でバックアップされており、管理センタ 1 6 0 から配布を受けるコンテンツ暗号鍵をタイマ 4 1 3 が所定の値に変化するまで記憶することができる。タイマ 4 1 3 は電池 4 1 4 でバックアップされており、管理センタ 1 6 0 から配布されたタイマの初期値から時間と共に変化し所定の値になるとコンテンツ暗号鍵記憶部 4 1 2 のデータをクリアする。

#### 【 0 0 8 7 】

復号部 4 0 3 は入出力部 4 0 2 を介して店舗のサーバ 1 6 2 あるいはユーザが所有する再生装置 1 7 0 からの暗号化データを受信すると制御部 4 0 1 の制御により、ＩＣカード秘密鍵、あるいは管理センタ公開鍵を使って暗号データを復号することができる。暗号部 4 0 4 は、入出力部 4 0 2 を介して店舗のサーバ 1 6 2 あるいはユーザが所有する再生装置 1 7 0 へデータを送信する時、制御部 1 6 0 の制御によりＩＣカード秘密鍵あるいは再生装置の公開鍵を使いデータを暗号化することができる。圧縮部 4 0 5 はハッシュ関数を用いて制御部 4 0 1 の制御により任意のデータの圧縮を行うことができる。乱数発生部 4 0 6 は制御部 4 0 1 の制御により乱数を発生することができる。認証部 4 0 7 は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行うことができる。

#### 【 0 0 8 8 】

図 2 0 は、図 1 6 に示す再生装置 1 7 0 の詳細な構成を示す図である。

再生装置 1 7 0 は制御部 5 0 1 と、I C カード入出力部 5 0 2 と、復号部 5 0 3 と、暗号部 5 0 4 と、圧縮部 5 0 5 と、乱数発生部 5 0 6 と、認証部 5 0 7 と、コンテンツ記録媒体入出力部 5 0 9 と、再生装置秘密鍵記憶部 5 1 0 と、管理センタ公開鍵記憶部 5 1 1 と、再生装置公開鍵証明書記憶部 5 1 2 と、タイマ 5 1 3 と、コンテンツ暗号鍵記憶部 5 1 4 と、コンテンツ鍵復号部 5 1 5 と、コンテンツ再生部 5 1 6 とで構成されている。

## 【 0 0 8 9 】

再生装置秘密鍵記憶部 5 1 0 には、再生装置 1 7 0 の秘密鍵が記憶されている。管理センタ公開鍵記憶部 5 1 1 は、管理センタ秘密鍵と所定の方法によってペアとなっている管理センタ公開鍵が記憶されている。再生装置公開鍵証明書記憶部 5 1 2 は管理センタ 1 6 0 が発行した再生装置公開鍵証明書が記憶されている。タイマ 5 1 3 は、制御部 5 0 1 が I C カード入出力部 5 0 2 を介して I C カード 1 6 7 から読み出されたレンタル期間を示す所定のタイマ値を書き込まれ、タイマ値は時間と共に変化しレンタル期間が終了する所定の値になるとコンテンツ暗号鍵記憶部 5 1 4 のデータをクリアする。コンテンツ暗号鍵記憶部 5 1 4 は、制御部 5 0 1 が I C カード入出力部 5 0 2 を介して I C カード 1 6 7 から読み出されたコンテンツ暗号鍵が記憶される。復号部 5 0 3 は I C カード入出力部 5 0 2 を介して I C カード 1 6 7 から暗号化データやデジタル証明データを受信すると制御部 5 0 1 の制御により、再生装置秘密鍵、あるいは管理センタ公開鍵を使って暗号データを復号することができる。

## 【 0 0 9 0 】

暗号部 5 0 4 は I C カード入出力部 5 0 2 を介して I C カード 1 6 7 からデータを送信する時、制御部 1 6 0 の制御により再生装置秘密鍵を使いデータを暗号化することができる。圧縮部 5 0 5 はハッシュ関数を用いて制御部 5 0 1 の制御により任意のデータの圧縮を行うことができる。乱数発生部 5 0 6 は制御部 5 0 1 の制御により乱数を発生することができる。認証部 5 0 7 は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行うことができる。

## 【 0 0 9 1 】

次に、再生装置 1 7 0 と I C カード 1 6 7 の相互認証の動作を図 2 1 に示すフローチャートを使用して説明する。

この相互認証は I C カード 1 6 7 と再生装置 1 7 0 の工場出荷前、ユーザが本システムを初めて利用する時、再生装置 1 7 0 の機種変更時、またはコンテンツ再生時にも行われる。

#### 【 0 0 9 2 】

まず、再生装置 1 7 0 へ I C カード 1 6 7 を接続する ( S 1 0 1 ) 。再生装置 1 7 0 の制御部 5 0 1 は I C カード入出力部 5 0 2 を介して I C カード 1 6 7 の接続を確認し、接続が認識されるまで処理を繰り返す ( S 1 0 2 ) 。再生装置 1 7 0 の制御部 5 0 1 は I C カード 1 6 7 の接続を確認すると、 I C カード 1 6 7 に対して再生装置公開鍵証明書記憶部 5 1 2 に記憶されている再生装置公開鍵証明書 PKpl, S1 と共に相互認証の要求を I C カード入出力部 5 0 2 を介して行う ( S 1 0 3 ) 。次に、 I C カード 1 6 7 の制御部 4 0 1 は入出力部 4 0 2 を介して再生装置公開鍵証明書 PKpl, S1 と共に相互認証の要求を受信すると、管理センタ公開鍵記憶部 4 0 9 に記憶されている管理センタ公開鍵 PKcnt を用いて再生装置公開鍵証明書の署名 S1 を復号部 4 0 3 にて復号し PKcnt ( S1 ) を生成し、圧縮部 4 0 5 にてハッシュ関数を用いて管理センタ公開鍵 PKpl を圧縮して H ( PKpl ) を生成し、認証部 4 0 7 にて PKcnt と H ( PKpl ) を照合する ( S 1 0 4 ) 。

#### 【 0 0 9 3 】

ステップ S 1 0 5 により PKcnt と H ( PKpl ) が不一致である場合、 I C カード 1 6 7 の制御部 4 0 1 は管理センタ 1 6 0 が発行していない不正な再生装置公開鍵証明書であると判断し、入出力部 4 0 2 を介して再生装置 1 7 0 へエラー通知を行う ( S 1 0 6 ) 。再生装置 1 7 0 の制御部 5 0 1 は、 I C カード入出力部 5 0 2 を介してエラー通知を受信すると ( S 1 0 7 ) 、相互認証を中止する ( S 1 2 9 ) 。

#### 【 0 0 9 4 】

ステップ S 1 0 5 により、 PKcnt と H ( PKpl ) が一致した場合、 I C カード 1 6 7 の制御部 4 0 1 は管理センタ 1 6 0 が発行した正当な再生装置公開鍵証明書と判断し、 I C カード公開鍵証明書記憶部 4 1 0 に記憶されている I C カード公開鍵証明書 ( PKic, S2 ) を再生装置 1 7 0 へ入出力部 4 0 2 を介して送信する ( S 1 0

8)。再生装置 1 7 0 の制御部 5 0 1 は IC カード入出力部 5 0 2 を介して IC カード公開鍵証明書(PKic, S2)を受信すると、管理センタ公開鍵記憶部 5 1 1 に記憶している管理センタ公開鍵PKcntを用いて署名 S2を復号部 5 0 3 にて復号し、PKcnt(S2)を生成し、圧縮部 5 0 5 にてハッシュ関数を用いて IC カード公開鍵PKplを圧縮しH(PKpl)を生成し、認証部 5 0 7 にてPKcnt(S2)とH(PKpl)を照合する(S 1 0 9)。ステップ S 1 1 0 により、PKcnt(S2)とH(PKpl)が不一致である場合、再生装置 1 7 0 の制御部 5 0 1 は管理センタ 1 6 0 が発行していない不正な IC カード公開鍵証明書と判断し相互認証を中止する(S 1 2 9)。

## 【 0 0 9 5 】

ステップ S 1 1 0 により、PKcnt(S5)とH(PKic)が一致した場合、再生装置 1 7 0 の制御部 5 0 1 は管理センタ 1 6 0 が発行した正当な公開鍵証明書と判断し、次に乱数発生部 5 0 6 で乱数Rplを生成する(S 1 1 1)。再生装置 1 7 0 の制御部 5 0 1 は IC カード公開鍵PKicを用いて乱数Rplを暗号部 5 0 4 にて暗号化し、PKic(Rpl)を生成し(S 1 1 2)、PKic(Rpl)を IC カード 1 6 7 へ IC カード入出力部 5 0 2 を介して送信する(S 1 1 3)。IC カード 1 6 7 の制御部 4 0 1 は入出力部 4 0 2 を介してPKic(Rpl)を受信すると、IC カード秘密鍵記憶部 4 0 8 に記憶している IC カード秘密鍵SKicを用いてPKic(Rpl)を復号部 4 0 3 にて復号し、DRplを生成する(S 1 1 4)。

## 【 0 0 9 6 】

次に、乱数発生部 4 0 6 で乱数Ricを生成し(S 1 1 5)、再生装置公開鍵PKplを用いて乱数Ricを暗号部 4 0 4 にて暗号化し、PKpl(Ric)を生成し(S 1 1 6)、PKpl(Ric)とDRplを入出力部 4 0 2 を介して再生装置 1 7 0 へ送信する(S 1 1 7)。再生装置 1 7 0 の制御部 5 0 1 は IC カード入出力部 5 0 2 からPKpl(Ric)とDRplを受信すると(S 1 1 8)、再生装置 1 7 0 が生成した乱数Rplと IC カード 1 6 7 が復号したDRplを認証部 5 0 7 で照合する(S 1 1 9)。ステップ S 1 1 9 によりRplとDRplが不一致である場合、再生装置 1 7 0 の制御部 5 0 1 は IC カード公開鍵とペアではない IC カード秘密鍵を保持した不正な IC カードと判断し相互認証を中止する(S 1 2 9)。

## 【 0 0 9 7 】

ステップ S 1 1 9 により、Rpl と DRpl が一致した場合、再生装置 1 7 0 の制御部 5 0 1 は IC カード 公開鍵 と ペア である IC カード 秘密鍵 を保持した正当な IC カード と判断し、再生装置 秘密鍵 記憶部 5 1 0 に記憶されている再生装置 秘密鍵 SKpl を用いて S 1 1 8 にて受信した PKpl (Ric) を復号部 5 0 3 で復号し DRic を生成し (S 1 2 0)、IC カード 入出力部 5 0 2 を介して IC カード 1 6 7 へ DRic を送信する (S 1 2 1)。IC カード 1 6 7 の制御部 4 0 1 は入出力部 4 0 2 から DRic を受信すると (S 1 2 2)、IC カード 1 6 7 が生成した乱数 Ric と再生装置で復号した DRic を認証部 4 0 7 で照合する (S 1 2 3)。ステップ S 1 2 3 により、Ric と DRic が不一致である場合、IC カード 1 6 7 の制御部 4 0 1 は入出力部 4 0 2 を介して再生装置 1 7 0 へエラー通知を行う (S 1 2 4)。再生装置 1 7 0 の制御部 5 0 1 は IC カード 入出力部 5 0 2 からエラー通知を受信すると (S 1 2 5)、相互認証を中止する (S 1 2 9)。

## 【 0 0 9 8 】

ステップ S 1 2 3 により Ric と DRic が一致した場合、IC カード 1 6 7 の制御部 4 0 1 は再生装置 公開鍵 証明書記憶部 4 1 1 の内容と、ステップ S 1 0 4 で受信した再生装置 公開鍵 証明書 (PKpl, S1) を比較する (S 1 2 6 A)。ステップ S 1 2 6 A により再生装置 公開鍵 証明書記憶部 4 1 1 の内容と、ステップ S 1 0 4 で受信した再生装置 公開鍵 証明書 (PKpl, S1) が異なる場合、ステップ S 1 0 4 で受信した再生装置 1 7 0 の公開鍵 証明書 (PKpl, S1) を再生装置 公開鍵 証明書記憶部 4 1 1 に記憶する (S 1 2 6 B)。ステップ S 1 2 6 A により再生装置 公開鍵 証明書記憶部 4 1 1 の内容と、ステップ S 1 0 4 で受信した再生装置 公開鍵 証明書 (PKpl, S1) が等しい場合、ステップ S 1 2 7 へ遷移する。

## 【 0 0 9 9 】

次に、IC カード 1 6 7 の制御部 4 0 1 は相互認証の正常終了を入出力部 4 0 2 を介して再生装置 1 7 0 へ通知し (S 1 2 7)、再生装置 1 7 0 の制御部 5 0 1 は IC カード 入出力部 5 0 2 を介して相互認証の正常終了を受信すると相互認証を終了する (S 1 2 8)。

## 【 0 1 0 0 】

次に、図 1 6 に示す IC カード 1 6 7 と管理センタ 1 6 0 の相互認証の動作を

図 2 2 に示すフローチャートを使用して説明する。

ユーザは IC カード 1 6 7 とコンテンツ記録媒体 1 6 6 を店舗のサーバ 1 6 2 へ持参し IC カード 1 6 7 とコンテンツ記録媒体 1 6 6 をサーバ 1 6 2 へ接続する (S 2 0 1)。サーバ 1 6 2 の制御部 3 0 1 は IC カード入出力部 3 0 2 を介して IC カード 1 6 7 の接続を確認すると (S 2 0 2)、IC カード 1 6 7 の相互認証を実施するため、制御部 3 0 1 は IC カード公開鍵証明書の読み出し要求を IC カード入出力部 3 0 3 を介して IC カード 1 6 7 へ通知する (S 2 0 3)。IC カード 1 6 7 の制御部 4 0 1 は入出力部 4 0 2 から IC カード 1 6 7 の公開鍵証明書の読み出し要求を受信すると、IC カード公開鍵証明書記憶部 4 1 0 に記憶されている IC カード公開鍵証明書 (PKic, S2) を入出力部 4 0 2 を介してサーバ 1 6 2 へ送信する (S 2 0 4)。

#### 【0101】

次に、サーバ 1 6 2 の制御部 3 0 1 は、IC カード入出力部 3 0 3 から IC カード公開鍵証明書 (PKic, S2) を受信すると、通信部 3 0 2 からネットワーク 1 6 4 を介して管理センタ 1 6 0 へ IC カード公開鍵証明書 (PKic, S2) と共に相互認証を要求する (S 2 0 5)。管理センタ 1 6 0 の制御部 2 0 1 は通信部 2 0 7 を介してサーバ 1 6 2 からの相互認証要求と IC カード公開鍵証明書 (PKic, S2) を受信すると (S 2 0 6)、公開鍵データベース 2 1 1 から IC カード公開鍵証明書 (PKic, S2) の IC カード公開鍵 PKic を検索し、IC カード公開鍵 PKic が有効であるか確認する (S 2 0 7)。

#### 【0102】

ステップ S 2 0 7 により IC カード公開鍵 PKic が不正あるいは失効している場合、管理センタ 1 6 0 の制御部 2 0 1 は相互認証要求の応答として通信部 2 0 7 からネットワーク 1 6 4 を介してサーバ 1 6 2 へエラー通知を送信し (S 2 0 8)、サーバ 1 6 2 の制御部 3 0 1 は通信部 3 0 2 を介してエラー通知を受信すると相互認証処理を中止する (S 2 3 0)。

ステップ S 2 0 7 により IC カード公開鍵 PKic が有効であると判断した場合、S 2 0 6 で受信した IC カード公開鍵証明書 (PKic, S2) の署名 S2 を管理センタ公開鍵記憶部 2 0 9 に記憶されている管理センタ公開鍵 PKcnt を用いて復号部 2



03にて復号し、PKcnt(S2)を生成し、PKicを圧縮部204にてハッシュ関数を用いて圧縮しH(PKic)を生成し、次に認証部206にてPKic(S2)とH(PKic)が等しいか照合する(S2081)。

【0103】

ステップS209によりPKic(S2)とH(PKic)が不一致の場合、管理センタ160の制御部201は管理センタ160が発行していない公開鍵証明書であると判断して通信部207からネットワーク164を介してサーバ162へエラーを通知し(S210)、サーバ162の制御部301はS210より通信部302を介してエラー通知を受信すると相互認証を中止する(S230)。

【0104】

ステップS209によりPKic(S2)とH(PKic)が一致した場合、管理センタ160の制御部201はステップS206で受信したICカード公開鍵証明書(PKic, S2)を管理センタ160が発行した公開鍵証明書であると判断して乱数発生部205で乱数Rcntを発生させ(S211)、ICカード公開鍵PKicを用いて暗号部203にて乱数Rcntを暗号化してPKic(Rcnt)を生成し(S212)、通信部207からネットワーク164を介してサーバ162へ相互認証要求の応答データとしてPKic(Rcnt)を送信する(S213)。サーバ162の制御部301を通信部から302から暗号データPKic(Rcnt)を受信すると、ICカード入出力部303を介してICカード167へPKic(Rcnt)を送信する(S214)。

【0105】

ICカード167の制御部401は、入出力部402からPKic(Rcnt)を受信すると、復号部403にてICカード秘密鍵記憶部408に記憶されているICカード秘密鍵をSKicを用いてPKic(Rcnt)を復号部403で復号し、DRcntを生成する(S215)。次に、ICカード167の制御部401は、乱数発生部406にて乱数Ricを発生し(S216)、暗号部404にて管理センタ公開鍵記憶部409に記憶されている管理センタ公開鍵PKcntを用いて暗号部404で暗号化し、PKcnt(Ric)を生成し(S217)、相互認証要求の応答データとしてPKic(Ric)とDRcntを入出力部402からサーバ162へ送信する(S218)。

【0106】

サーバ162の制御部301はICカード入出力部303からPKic(Ric)とDRcntを受信すると、相互認証要求の応答データとして通信部302からネットワーク164を介して管理センタ160へ、PKcnt(Ric)とDRcntを送信する(S219)。管理センタ160の制御部201は通信部207からPKcnt(Ric)とDRcntを受信すると(S220)、認証部206にて復号データDRcntと乱数データRcntを照合する(S221)。ステップS221によりDRcntとRcntが不一致である場合、管理センタ160の制御部201はICカード公開鍵PKicのペアであるICカード秘密鍵を保持していない不正なICカードと判断し、通信部207からネットワーク164を介してサーバ162へエラー通知し(S222)、サーバ162の制御部301は通信部302からエラー通知を受信すると相互認証を中止する(S230)。

#### 【0107】

ステップS221によりDRcntとRcntが一致する場合、管理センタ160の制御部201は、ICカード公開鍵PKicのペアであるICカード秘密鍵を保持している正当なICカードと判断し、復号部202にて管理センタ秘密鍵記憶部208に記憶している管理センタ秘密鍵SKcntを用いてPKcnt(Ric)を復号しDRicを生成し、通信部207からネットワーク164を介してサーバ162へDRicを送信する(S223)。サーバ162の制御部301は通信部302からDRicを受信すると、ICカード入出力部303を介してICカード167へDRicを送信する(S224)。次に、ICカード167の制御部401は入出力部402を介してサーバ162からDRicを受信すると(S225)、乱数RicとDRicを認証部407にて照合する(S226)。

#### 【0108】

ステップS226により、乱数RicとDRicが不一致である場合、ICカード167の制御部401は管理センタ秘密鍵SKcntを保持していない不正な相手と判断し、入出力部402からサーバ162へエラー通知し(S227)、サーバ162の制御部301はICカード入出力部303からエラー通知を受信すると相互認証を中止する。ステップS226により、Ricと復号データDRicが一致した場合、ICカード167の制御部401は管理センタが秘密鍵SKcntを保持してい

る正当な管理センタであると判断し、入出力部402からサーバ162へ正常終了の通知を送信し(S228)、サーバ162の制御部301はICカード入出力部303から正常終了の通知を受信すると相互認証を正常終了する(S229)。

#### 【0109】

図23は、上述したICカード167と管理センタ160の相互認証の終了後におけるICカード167から管理センタ160への再生装置公開鍵証明書の転送処理を示している。

まず、サーバ162の制御部301はICカード入出力部303からICカード167へ再生装置公開鍵証明書の読み出し要求する(S301)。ICカード167の制御部401は入出力部402を介してサーバ162から再生装置公開鍵証明書の読み出し要求を受信すると、再生装置公開証明書記憶部411に記憶している再生装置公開鍵証明書(PKpl, S1)を入出力部402からサーバ162へ送信する(S302)。サーバ162の制御部301は、ICカード入出力部303から再生装置公開鍵証明書(PKpl, S1)を受信すると、通信部302からネットワーク164を介して管理センタ160へ再生装置公開鍵証明書(PKpl, S1)を送信する(S304)。管理センタ160の制御部201は通信部207を介してサーバ162から再生装置公開鍵証明書(PKpl, S1)を受信すると(S305)、公開鍵データベース211を検索し、有効な公開鍵であるか検証する(S306)。

#### 【0110】

ステップS306によりステップS305で受信した再生装置公開鍵証明書が不正あるいは失効している場合、管理センタ160の制御部201は通信部207からネットワークを介してサーバ162へエラー通知をし(S307)、サーバ162の制御部301は通信部302からエラー通知を受信すると、再生装置公開鍵証明書の転送処理を中止する(S312)。ステップS306によりステップS305で受信した再生装置公開鍵証明書が正当であると判断した場合、復号部202にて管理センタ公開鍵記憶部209に記憶している管理センタ公開鍵PKcntを用いて再生装置公開鍵証明書(PKpl, S1)の署名S1を復号部202で復号し、PKcnt(S1)を生成し、圧縮部にてハッシュ関数を用いて再生装置公開鍵証明書(PKpl, S1)のPKplを圧縮部204で圧縮してH(PKpl)を生成し、PKpl(S1)とH(PKpl

)を認証部 2 0 6 にて照合する(S 3 0 8)。

#### 【 0 1 1 1 】

ステップ S 3 0 9 の判断において PKpl(S1)と H(PKpl)が不一致であった場合、管理センタ 1 6 0 の制御部 2 0 1 は再生装置公開鍵 PKpl とペアである再生装置秘密鍵 SKpl を保持しない不正な再生装置と判断し、通信部 2 0 7 からネットワーク 1 6 4 を介してサーバ 1 6 2 へエラー通知を送信し(S 3 1 0)、サーバ 1 6 2 の制御部 3 0 1 は通信部 3 0 2 からエラー通知を受信すると再生装置公開鍵証明書の転送処理を中止する(S 3 1 2)。ステップ S 3 0 9 の判断において、PKpl(S1)と H(PKpl)が一致した場合、管理センタ 1 6 0 の制御部 2 0 1 は再生装置公開鍵 PKpl とペアである再生装置秘密鍵 SKpl を保持した正当な再生装置と判断し、通信部 2 0 2 からネットワーク 1 6 4 を介してサーバ 1 6 2 へ正常終了通知し(S 3 1 0)、サーバ 1 6 2 の制御部 3 0 1 は通信部 3 0 2 から正常終了の通知を受信すると再生装置公開鍵証明書の転送処理を正常終了する(S 3 1 1)。

#### 【 0 1 1 2 】

図 2 4 は、上述した再生装置公開鍵証明書の転送処理の後、コンテンツの再生に必要な情報のダウンロード処理のフローチャートを示している。

まず、ユーザはサーバ 1 6 2 の表示部 3 0 6 からレンタルするコンテンツを選択し、入力部 3 0 5 にてコンテンツのタイトル C とレンタル期間 T を入力する(S 4 0 1)。コンテンツのタイトル C とレンタル期間 T を含む契約内容を CT として、サーバ 1 6 2 の制御部 3 0 1 は契約内容 CT と共に契約データ作成要求を IC カード入出力部 3 0 3 を介して IC カード 1 6 7 へ送信する(S 4 0 2)。IC カード 1 6 7 の制御部 4 0 1 は入出力部 4 0 2 から契約データ作成要求と契約内容 CT を受信すると、契約内容 CT を圧縮部 4 0 5 にてハッシュ関数を用いて圧縮し、H(CT)を生成し、IC カード秘密鍵記憶部 4 0 8 に記憶している IC カード秘密鍵 SKic を用いて H(CT)を暗号部 4 0 4 で暗号化し、署名 S3 を生成する(S 4 0 3)。

#### 【 0 1 1 3 】

次に、IC カード 1 6 7 の制御部 4 0 1 は、入出力部 4 0 2 を介して契約データ CT と署名 S3 をサーバ 1 6 2 へ送信する(S 4 0 4)。サーバ 1 6 2 の制御部 3 0 1 は IC カード入出力部 3 0 3 から契約データ CT と署名 S3 を受信すると、通

信部 3 0 2 からネットワーク 1 6 4 を介して管理センタ 1 6 0 へ契約データ CT と署名 S 3 と共にコンテンツ鍵のダウンロード要求を送信する (S 4 0 5)。管理センタ 1 6 0 の制御部 2 0 1 は通信部 2 0 7 からコンテンツ暗号鍵ダウンロード要求と契約データ CT と署名 S 3 を受信すると (S 4 0 6)、復号部 2 0 2 にて、前述した相互認証によって正常と確認された IC カードの公開鍵 PKic を用いて S 3 を復号部 2 0 2 で復号し PKic (S 3) を生成し、圧縮部 2 0 4 にてハッシュ関数を用いて契約データ CT を圧縮して H (CT) を生成し、認証部 2 0 6 にて PKic (S 3) と H (CT) を照合する (S 4 0 7)。

## 【 0 1 1 4 】

ステップ S 4 0 8 から、PKic (S 3) と H (CT) が不一致である場合、管理センタ 1 6 0 の制御部 2 0 1 は IC カード 1 6 7 が不正かあるいはデータが改竄されたと判断し通信部 2 0 7 からネットワーク 1 6 4 を介してサーバ 1 6 2 へエラー通知 (S 4 0 9)、サーバ 1 6 2 の制御部 3 0 1 は通信部 3 0 2 からエラー通知を受信するとコンテンツ暗号鍵ダウンロード処理を中止する (S 4 2 6)。ステップ S 4 0 8 において、PKic (S 3) と H (CT) が一致した場合、管理センタ 1 6 0 の制御部 2 0 1 は契約データ CT の発行者を IC カード 1 6 7 と特定し、かつ、データに改竄を加えられてはいないと判断し、課金データベース 2 1 2 へ契約内容 CT を書き込む (S 4 1 0)。

## 【 0 1 1 5 】

次に、管理センタ 1 6 0 の制御部 2 0 1 は、コンテンツ鍵記憶部 2 1 0 に記憶している契約内容 CT のコンテンツのタイトルに対応したコンテンツ暗号鍵 CK を読み出し、圧縮部 2 0 4 にてハッシュ関数を用いて圧縮して H (CK) を生成し、暗号部 2 0 3 にて管理センタ公開鍵記憶部 2 0 8 に記憶している管理センタ秘密鍵 SK<sub>cnt</sub> を用いて H (CK) を暗号部 2 0 3 で暗号化し、署名 S 4 を生成する (S 4 1 1)。次に、暗号部 2 0 3 にて、再生装置公開鍵 PKpl を用いて、コンテンツ暗号鍵 CK と署名 S 4 を暗号化し PKpl (CK, S 4) を生成する (S 4 1 2)。次に、圧縮部 2 0 4 にてハッシュ関数を用いて PKpl (CK, S 4) と契約データ CT を圧縮し H (PKpl (CK, S 4), CT) を生成し、暗号部 2 0 3 にて IC カード公開鍵 PKic を用いて、H (PKpl (CK, S 4), CT) を暗号化し署名 S 5 を生成する (S 4 1 3)。

## 【 0 1 1 6 】

次に、暗号部 2 0 3 にて I C カード公開鍵 PKic を用いて、暗号化されたコンテンツ暗号鍵 PKpl (CK, S4) と契約データ CT と署名 S5 を暗号化し PKic (PKpl (CK, S4), CT, S5) を生成する (S 4 1 4)。次に、コンテンツ鍵ダウンロード要求に対するコンテンツ鍵データとして PKic (PKpl (CK, S4), CT, S5) を通信部 2 0 7 からネットワーク 1 6 4 を介してサーバ 1 6 2 へ送信する (S 4 1 5)。

## 【 0 1 1 7 】

サーバ 1 6 2 の制御部 3 0 1 は通信部 3 0 2 からコンテンツ鍵データ PKic (PKpl (CK, S4), CT, S5) を受信すると、I C カード入出力部 3 0 3 を介して I C カード 1 6 7 へコンテンツ鍵データ PKic (PKpl (CK, S4), CT, S5) と共にコンテンツ鍵記憶要求を送信する (S 4 1 6)。I C カード 1 6 7 の制御部 4 0 1 は入出力部 4 0 2 からコンテンツ鍵記憶要求とコンテンツ鍵データ PKic (PKpl (CK, S4), CT, S5) を受信すると、復号部 4 0 3 にて I C カード秘密鍵記憶部 4 0 8 に記憶している I C カード秘密鍵 SKic を用いて PKic (PKpl (CK, S4), CT, S5) を復号し PKpl (CK, S4) と CT と S5 を生成する (S 4 1 7)。次に、復号部 4 0 3 にて管理センタ公開鍵記憶部 4 0 9 に記憶している管理センタ公開鍵 PKcnt を用いて署名 S5 を復号し PKcnt (S5) を生成し、圧縮部 4 0 5 にてハッシュ関数を用いて PKpl (CK, S4) と CT を圧縮し H (PKpl (CK, S4), CT) を生成し、認証部 4 0 7 にて PKcnt (S5) と H (PKpl (CK, S4), CT) を照合する (S 4 1 8)。

## 【 0 1 1 8 】

ステップ S 4 1 9 から PKcnt (S5) と H (PKpl (CK, S4), CT) が不一致である場合、I C カード 1 6 7 の制御部 4 0 1 は、不正なデータかあるいはデータに改竄を加えたと判断し、入出力部 4 0 2 を介してサーバ 1 6 2 へエラー通知を送信し (S 4 2 0)、サーバ 1 6 2 の制御部 3 0 1 は I C カード入出力部 3 0 3 からエラー通知を受信するとコンテンツ暗号鍵ダウンロード処理を中止する (S 4 2 6)。ステップ S 4 1 9 の判断において、PKcnt (S5) と H (PKpl (CK, S4), CT) が一致した場合、I C カード 1 6 7 の制御部 4 0 1 はデータの発行者を管理センタ 1 6 0 と特定し、かつ、データに改竄がないと判断し、契約内容 CT の契約期限データ T をタイマ 4 1 3 へセットし (S 4 2 1)、暗号化コンテンツ鍵 PKpl (CK, S4) をコンテン

ツ鍵記憶部 4 1 2 へセットする (S 4 2 2)。

【 0 1 1 9 】

次に、ICカード 1 6 7 の制御部 4 0 1 は、入出力部 4 0 2 を介してサーバ 1 6 2 へコンテンツ鍵記憶要求に対しての正常応答を送信し (S 4 2 3)、サーバ 1 6 2 の制御部 3 0 1 は、ICカード入出力部 3 0 3 から正常終了を受信するとコンテンツ記憶部 3 0 7 からコンテンツデータをコンテンツ記憶媒体 1 6 6 へ書き込む (S 4 2 4)。コンテンツ記録媒体 1 6 6 へのコンテンツデータの書き込みが終了するとユーザはICカード 1 6 7 とコンテンツ記録媒体 1 6 6 を持ち帰る (S 4 2 5)。

【 0 1 2 0 】

図 2 5 は、図 1 6 の再生装置 1 7 0 においてコンテンツを再生する処理のフローチャートを示している。まず、ユーザは再生装置 1 7 0 へコンテンツ記録媒体 1 6 6 およびICカード 1 6 7 を接続し、再生装置 1 7 0 とICカード 1 6 7 は前述した手順による相互認証を行う (S 5 0 1)。再生装置 1 7 0 の制御部 5 0 1 は操作入力部 5 0 8 からのコンテンツの再生指示 (S 5 0 2) により、ICカード入出力部 5 0 2 を介してICカード 1 6 7 へコンテンツ暗号鍵の送信を要求する (S 5 0 3)。ICカード 1 6 7 の制御部 4 0 1 は、入出力部 4 0 2 からコンテンツ暗号鍵の送信要求を受信すると (S 5 0 4)、コンテンツ暗号鍵記憶部 4 1 2 を読み出し、データが存在しているか確認する (S 5 0 5)。

【 0 1 2 1 】

ステップ S 5 0 5 の判断において、コンテンツ暗号鍵記憶部 4 1 2 のデータが消去されていた場合、ICカード 1 6 7 の制御部 4 0 1 は入出力部 4 0 2 を介して再生装置 1 7 0 へコンテンツ暗号鍵の消去通知を送信し (S 5 0 6)、再生装置 1 7 0 の制御部 5 0 1 はコンテンツ暗号鍵の消去通知を受信するとコンテンツ再生不可としてコンテンツ再生処理を終了する (S 5 2 0)。ステップ S 5 0 5 の判断において、コンテンツ暗号鍵記憶部 4 1 2 のデータが保持されている場合、ICカード 1 6 7 の制御部 4 0 1 はタイマ 4 1 3 からタイマ値  $t$  を読み出し (S 5 0 8)、圧縮部 4 0 5 にてハッシュ関数を用いて暗号化されたコンテンツ暗号鍵  $PK_{pl}(CK, S4)$  とタイマ値  $t$  を圧縮して  $H(PK_{pl}(CK, S4), t)$  を生成し、暗号部 4

04にてICカード秘密鍵記憶部410に記憶されているICカード秘密鍵SKicを用いて $H(PKpl(CK, S4), t)$ を暗号化し、署名S6を生成する(S509)。

#### 【0122】

次に、ICカード167の制御部401は、暗号化されたコンテンツ暗号鍵PKpl(CK, S4)とタイマ値tと署名S6を入出力部402を介して再生装置170へ送信する(S510)。再生装置170の制御部501は、ICカード入出力部から暗号化されたコンテンツ暗号鍵PKpl(CK, S4)とタイマ値tと署名S6を受信すると、復号部503にてICカード公開鍵PKicを用いて署名S6を復号してPKic(S6)を生成し、圧縮部505にてハッシュ関数を用いてコンテンツ暗号鍵PKpl(CK, S4)とタイマ値tを圧縮し、 $H(PKpl(CK, S4), t)$ を生成し、認証部507にてPKic(S6)と $H(PKpl(CK, S4), t)$ を照合する(S511)。ステップS512よりPKic(S6)と $H(PKpl(CK, S4), t)$ が不一致であった場合、再生装置170の制御部501は不正データかデータに改竄があったと判断し、再生不可として再生処理を終了する(S520)。

#### 【0123】

ステップS512よりPKic(S6)と $H(PKpl(CK, S4), t)$ が一致した場合、再生装置170の制御部501はタイマ値tをタイマ513へセット(S513)する。次に、再生装置170の制御部501は、復号部503にて再生装置秘密鍵記憶部509に記憶されている再生装置秘密鍵SKplを用いて暗号化されたコンテンツ暗号鍵PKpl(CK, S4)を復号しCKと署名S4を生成する(S514)。次に、復号部503にて管理センタ公開鍵記憶部511に記憶されている管理センタ公開鍵PKcntを用いて署名S4を復号しPKcnt(S4)を生成し、圧縮部505にてハッシュ関数を用いてCKを圧縮しH(CK)を生成し、認証部507でPKcnt(S4)とH(CK)を照合する(S515)。ステップS516よりPKcnt(S4)とH(CK)が不一致である場合、再生装置170の制御部501は管理センタ160が発行したデータではないかあるいはデータが改竄されたと判断し、再生不可として再生処理を終了する(S520)。

#### 【0124】

ステップS516よりPKcnt(S4)とH(CK)が一致した場合、再生装置170の



制御部 5 0 1 はコンテンツ暗号鍵CKをコンテンツ暗号鍵記憶部 5 1 4 へセットする (S 5 1 7)。次に、再生装置 1 7 0 の制御部 5 0 1 はコンテンツ記録媒体入出力部 5 0 9 を介してコンテンツ記録媒体 1 6 6 からコンテンツデータを読み出し、コンテンツ復号部 5 1 5 にてコンテンツ暗号鍵記憶部 5 1 4 のコンテンツ暗号鍵CKを用いてコンテンツデータを復号し (S 5 1 8)、コンテンツ再生を行う (S 5 1 9)。

#### 【 0 1 2 5 】

次に、上述した図 1 6 の構成の利点を説明する。

- (1) 再生装置の公開鍵証明書を I C カードへ記憶することで再生可能な再生装置を安全に限定することかできる。
- (2) コンテンツをレンタルする前に、再生装置の公開鍵証明書を I C カードへ記憶することで、再生装置の機種を安全かつ柔軟に変更することが可能であり、変更後の再生装置に対して再生を安全に限定できる。
- (3) 再生に必要なコンテンツ暗号鍵、再生期限情報及び公開鍵証明書は管理センタが発行したデータのみ有効となるので、データは一元的に保証され安全なコンテンツの流通が可能になる。
- (4) I C カードの内部に再生期限情報を記憶し、リアルタイムに再生期限を減ずる機能を有することで、再生期限の改竄を防止することができる。
- (5) I C カードならびに再生装置の内部に再生期限を過ぎるとコンテンツ再生に必要なコンテンツ暗号鍵を消去する機能を有することで、耐タンパ性を向上することができる。

#### 【 0 1 2 6 】

#### < 第 4 実施形態 >

次に、この発明の第 4 の実施形態について図 2 6 ～図 2 9 を参照して説明する。この実施形態においては、R H D D が記録媒体だけでなく、読出／書込回路および制御回路をも含んで構成されている。

#### 【 0 1 2 7 】

図 2 6 は同実施形態によるコンテンツレンタルシステムの構成を示すブロック図である。この図において、7 0 1 はレンタル店に設けられる店舗サーバである

。702は複数の店舗サーバ701を統括管理するセンタサーバであり、インターネット703を介して各店舗サーバ701に接続されている。このセンタサーバ702が各レンタル店を統括する管理センタに設けられている。そして、この管理センタが図1のビデオソフトデュプリケータに相当する。704はユーザが所有するRHDDであり、ユーザはこのRHDD704を店舗サーバ701にセットしてコンテンツのダウンロードを受け、自宅に戻り、RHDD704を再生装置705にセットしてコンテンツの再生を行う。

## 【0128】

図27は、店舗サーバ701の構成を示すブロック図である。この図において、711はCPU（中央処理装置）、712はメモリ、713はCPU711、メモリ712およびPCI（Peripheral Component Interconnect）バス714を相互に接続するブリッジ回路である。716はマスター磁気ディスク装置であり、センタサーバ702（図26）からインターネット703を介して供給されるコンテンツおよびディスクコマンドが記憶される。717はマスター磁気ディスク装置716をPCIバス714に接続するIDE（Integrated Drive Electronics）インターフェイスである。718はPCIバス714と、RHDD704が接続される端子719とを接続するブリッジ回路である。

## 【0129】

図28はRHDD704の構成を示すブロック図である。この図において、721はCPU、722はシリアルインターフェイス、723は店舗サーバ701の端子719または再生装置705の端子734（図29）に接続される端子である。724は店舗サーバ701から読み出されるコンテンツおよびディスクコマンドが記憶される磁気ディスク装置、725はIDEインターフェイス、726はI/F（インターフェイス）切替用バッファである。また、727は電池728によってバックアップされたりアルタイムクロック、729はICカードである。

## 【0130】

図29は再生装置705の構成を示すブロック図である。この図において、731はCPU、732は不揮発性メモリ、733はシリアルインターフェイス、

734はRHDD704の端子723に接続される端子である。また、735はIDEインターフェイス、736は、端子734に接続されたRHDD704からIDEインターフェイス735を介して供給される暗号化されたコンテンツおよびディスクコマンドを復号する復号化回路、705は復号化回路736とMP EGデコーダ738とを接続するI/O回路である。MP EGデコーダ738は、MP EG規格に基づいて圧縮されたデータを元のデータに伸長するデコーダ、グラフィック制御回路739はMP EGデコーダ738から出力されるデータに基づいて表示装置740に画像表示を行う制御回路である。

#### 【0131】

次に、上記実施形態の動作を説明する。

まず、センタサーバ702（図26）は、インターネット703を介して店舗サーバ701へコンテンツおよびディスクコマンドを配信すると共に、コンテンツのダウンロード可能回数を配信する。ここで、配信されるコンテンツは、予めセンタサーバ702において暗号化され、かつ、MP EG規格によって圧縮されている。配信されたコンテンツ、ディスクコマンドおよびダウンロード可能回数は店舗サーバ701（図27）のPCIバス714、IDEインターフェイス717を介してマスター磁気ディスク装置716に記憶される。

#### 【0132】

一方、ユーザはRHDD704および再生装置705をセットで購入する。この購入時において、RHDD704のICカード729にユーザ（購入者）の属性情報（氏名、承認番号、課金情報、住所、電話番号など）が記憶される。なお、ICカードが備わっていないRHDDの場合は、この属性情報が磁気ディスク装置724に記憶される。また、このICカード729には、予め、再生装置705の識別番号が記憶されており、また、再生装置705のメモリ732にも、同じ識別番号が記憶されている。そして、ユーザは、RHDD704を持参してレンタル業者の店舗へ出向き、係員の指示に従ってその店舗に設置されている店舗サーバ701にRHDD704をセットする。

#### 【0133】

RHDD704がセットされると、RHDD704のCPU721がICカー

ド 7 2 9 内のユーザ属性情報を読み出し、店舗サーバ 7 0 1 へ出力する。この属性情報は、ブリッジ回路 7 1 8、P C I バス 7 1 4、ブリッジ回路 7 1 3 を介してメモリ 7 1 2 に記憶される。C P U 7 1 1 はこの属性情報をインターネット 7 0 3 を介してセンタサーバ 7 0 2 へ送信する。センタサーバ 7 0 2 は、送信された属性情報に基づいてレンタルの可否および料金体系を判定し、その結果を店舗サーバ 7 0 1 へ送信する。

## 【 0 1 3 4 】

次に、店舗サーバ 7 0 1 の C P U 7 1 1 は、上記センタサーバ 7 0 2 からの送信内容がレンタル可であった場合に、表示画面（図示略）にマスター磁気ディスク装置 7 1 6 内のコンテンツの一覧表を表示する。そして、ユーザが一覧表の中からダウンロードを希望するコンテンツを選択すると、選択されたコンテンツがマスター磁気ディスク装置 7 1 6 から読み出され、R H D D 7 0 4 の磁気ディスク装置 7 2 4 に書き込まれる。次に、C P U 7 1 1 が、復号鍵をメモリ 7 1 2 から読み出し、R H D D 7 0 4 へ出力し、次いで、再生期限を演算し、R H D D 7 0 4 へ出力する。復号鍵は I C カード 7 2 9 に書き込まれ、また、再生期限は磁気ディスク装置 7 2 4 に書き込まれる。

## 【 0 1 3 5 】

次に、C P U 7 1 1 が、メモリ 7 1 2 に予め設定されている、ダウンロードしたコンテンツのダウンロード回数カウントエリアに「1」を加算する。このカウントエリア内の数値がそのコンテンツのダウンロード回数を示している。次いで、C P U 7 1 1 は該カウントエリア内の数値と、マスター磁気ディスク装置 7 1 6 内のダウンロード可能回数とを比較する。そして、カウントエリア内の数値がダウンロード可能回数を越えた場合は以後ダウンロードを禁止するとともに、その旨をセンタサーバ 7 0 2 に通知する。

## 【 0 1 3 6 】

店舗サーバ 7 0 1 においてコンテンツのダウンロードを受けたユーザは、R H D D 7 0 4 を自宅へ持ち帰り、再生装置 7 0 5 にセットし、再生スタートボタン（図示略）を押す。再生スタートボタンが押されると、R H D D 7 0 4 の C P U 7 2 1 は、まず、I C カード 7 2 9 内の識別番号を読み出し、再生装置 7 0 5 へ

出力する。この識別番号はシリアルインターフェイス 7 3 3 を介して CPU 7 3 1 へ供給される。CPU 7 3 1 はこの識別番号と、メモリ 7 3 2 内に予め設定されている自身の識別番号とを比較する。そして、一致していれば、以下に述べるコンテンツ再生処理に進むが、一致していない場合は、警報を発し、コンテンツ再生処理を行わない。

#### 【 0 1 3 7 】

RHDD 7 0 4 の CPU 7 2 1 は、上述した識別番号を出力した後、磁気ディスク装置 7 2 4 から再生期限を読み出し、リアルタイムクロック 7 2 7 から出力されている現在時刻と比較する。そして、現在時刻が再生期限を過ぎている場合は警報を発し、以後の処理を中止する。過ぎていなかった場合は、次に、ICカード 7 2 8 から復号鍵を読み出し、再生装置 7 0 5 へ出力する。この復号鍵は、IDE インターフェイス 7 3 5 を介して復号化回路 7 3 6 にセットされる。

以後、RHDD 7 0 4 の磁気ディスク装置 7 2 4 からコンテンツが順次読み出され、再生装置 7 0 5 へ出力される。再生装置 7 0 5 へ出力されたコンテンツは、復号化回路 7 3 6 において、復号鍵を用いて復号され、I/O 回路 7 0 5 を介して MPEG デコーダ 7 3 8 へ入力され、ここで、伸長され、グラフィック制御回路 7 3 9 を介して表示装置 7 4 0 において表示される。

#### 【 0 1 3 8 】

なお、上述した実施形態において、ユーザが何らかの方法で、識別番号の異なる再生装置によって RHDD 内のコンテンツの再生を行った場合、RHDD 内の磁気ディスク装置に再生装置の識別番号を記憶させ、そのユーザが次回店舗サーバに RHDD をセットした時、店舗サーバが上記識別番号から異なる再生装置による再生を検出し、ダウンロードを行わないようにしてもよい。

また、再生期限の管理において、期限が経過した場合に、RHDD 7 0 4 の CPU 7 2 1 が IC カード 7 2 9 内の復号鍵を消去してもよい。また、再生装置 7 0 5 内にリアルタイムクロックを設け、RHDD 7 0 4 から再生期限を出力させて再生装置 7 0 5 内において再生期限チェックをしてもよい。

#### 【 0 1 3 9 】

また、ユーザがコンテンツのダウンロードを受けた時、同時に、再生可能回数

を磁気ディスク装置 724 に記憶させ、再生回数が再生可能回数以上となった時再生を不能とするようにしてもよい。この場合、再生回数の判定方法は種々あるが、例えば、コンテンツの中間から後半部に再生マーカを設けておき、この再生マーカを経過してコンテンツを再生した場合に、1 回の再生としてカウントする。また、再生マーカはコンテンツのどこに設けてもよい。例えば、コンテンツの最初と最後にマーカを設けておき、この両方のマーカを通過した時のみカウントするようにしてもよい。また、コンテンツの先頭にのみマーカを設けておき、最初の部分さえ再生したら 1 回とカウントしてもよい。

## 【0140】

## 【発明の効果】

請求項 1 に記載の発明によれば次の効果を得ることができる。

(1) ビデオ貸し出し事業者が抱える不良在庫と機会損失という二律背反の問題を解決することができる。

(2) 映像製作会社には本流通システムを通して顧客から徴収されるレンタル料金の一部が貫流するため、従来よりも高い売上高を得ることもできる。

(3) レンタル用ビデオテープがセルビデオ市場へ低価格で流出することを防止できる。

## 【0141】

請求項 2 に記載の発明によれば、従来とは異なり常に新しい CM 情報を貸し出し用記録媒体に挿入し、顧客に視聴させることができ、従来の挿入 CM に比較すると、高い CM 効果を期待できる。また、この CM は新たな収入源となり、ビデオソフトメーカーと貸し出し事業者の経営が安定化する。また、顧客にとっても利益のある広告システムを享受することができる。

## 【0142】

請求項 4 ～請求項 8 に記載の発明によれば、ある期間が経過するとコンテンツの再生に必要な情報が消えてしまうため、コンテンツの再生が不可能になる。従って、レンタルシステムに適用した場合、コンテンツ媒体を返却しなくてもよいレンタルシステムの構築が可能となる。また、タイマを備えた場合、コンテンツの再生に必要な情報が消えるまでの期間を正確に設定することができる。

請求項 9 ～ 請求項 1 9 に記載の発明によれば、不正コピーによるデジタル映像情報の流出やビデオ市場の混乱を防止することができる。

【図面の簡単な説明】

- 【図 1】 この発明の実施形態の構成を示すブロック図である。
- 【図 2】 同実施形態の変形例を示すブロック図である。
- 【図 3】 図 1 または図 2 の実施形態における RHDD（リムーバブル磁気ディスク装置）の構成例を示すブロック図である。
- 【図 4】 図 3 に示す RHDD の動作を説明するためのフローチャートである。
- 【図 5】 図 3 に示す RHDD を再生装置に接続した状態を示すブロック図である。
- 【図 6】 図 5 に示す RHDD の再生時の動作を説明するためのブロック図である。
- 【図 7】 RHDD の他の構成例を示すブロック図である。
- 【図 8】 図 7 に示す RHDD の動作を説明するためのブロック図である。
- 【図 9】 RHDD のさらに他の構成例を示すブロック図である。
- 【図 1 0】 RHDD のさらに他の構成例を示すブロック図である。
- 【図 1 1】 RHDD のさらに他の構成例を示すブロック図である。
- 【図 1 2】 図 1 1 に示す RHDD の動作を説明するためのブロック図である。
- 【図 1 3】 図 1 1 に示す RHDD の動作を説明するためのブロック図である。
- 【図 1 4】 RHDD のさらに他の構成例を示すブロック図である。
- 【図 1 5】 図 1 4 における再生装置を他の構成例による再生装置に置き換えた構成を示すブロック図である。
- 【図 1 6】 この発明の他の実施形態の構成を示すブロック図である。
- 【図 1 7】 図 1 6 の実施形態における管理センタ 1 6 0 の構成を示すブロック図である。
- 【図 1 8】 図 1 6 の実施形態におけるサーバ 1 6 2 の構成を示すブロック

図である。

【図 1 9】 図 1 6 の実施形態における I C カード 1 6 7 の構成を示すブロック図である。

【図 2 0】 図 1 6 の実施形態における再生装置 1 7 0 の構成を示すブロック図である。

【図 2 1】 図 1 6 に示す実施形態における再生装置 1 7 0 と I C カード 1 6 7 の相互認証の動作を示すフローチャートである。

【図 2 2】 図 1 6 に示す実施形態における管理センタ 1 6 0 と I C カード 1 6 7 の相互認証の動作を示すフローチャートである。

【図 2 3】 図 1 6 に示す実施形態において、I C カード 1 6 7 から管理センタ 1 6 0 への再生装置公開鍵証明書 of 転送処理を示すフローチャートである。

【図 2 4】 図 1 6 に示す実施形態において、コンテンツのダウンロード処理を示すフローチャートである。

【図 2 5】 図 1 6 に示す実施形態において、コンテンツの再生処理を示すフローチャートである。

【図 2 6】 この発明のさらに他の実施形態の全体構成を示すブロック図である。

【図 2 7】 図 2 6 における店舗サーバ 7 0 1 の構成を示すブロック図である。

【図 2 8】 図 2 6 における R H D D 7 0 4 の構成を示すブロック図である。

【図 2 9】 図 2 6 における再生装置 7 0 5 の構成を示すブロック図である。

【図 3 0】 従来のビデオテープレンタルシステムの構成を示すブロック図である。

【図 3 1】 従来のビデオテープレンタルシステムの構成を示すブロック図である。

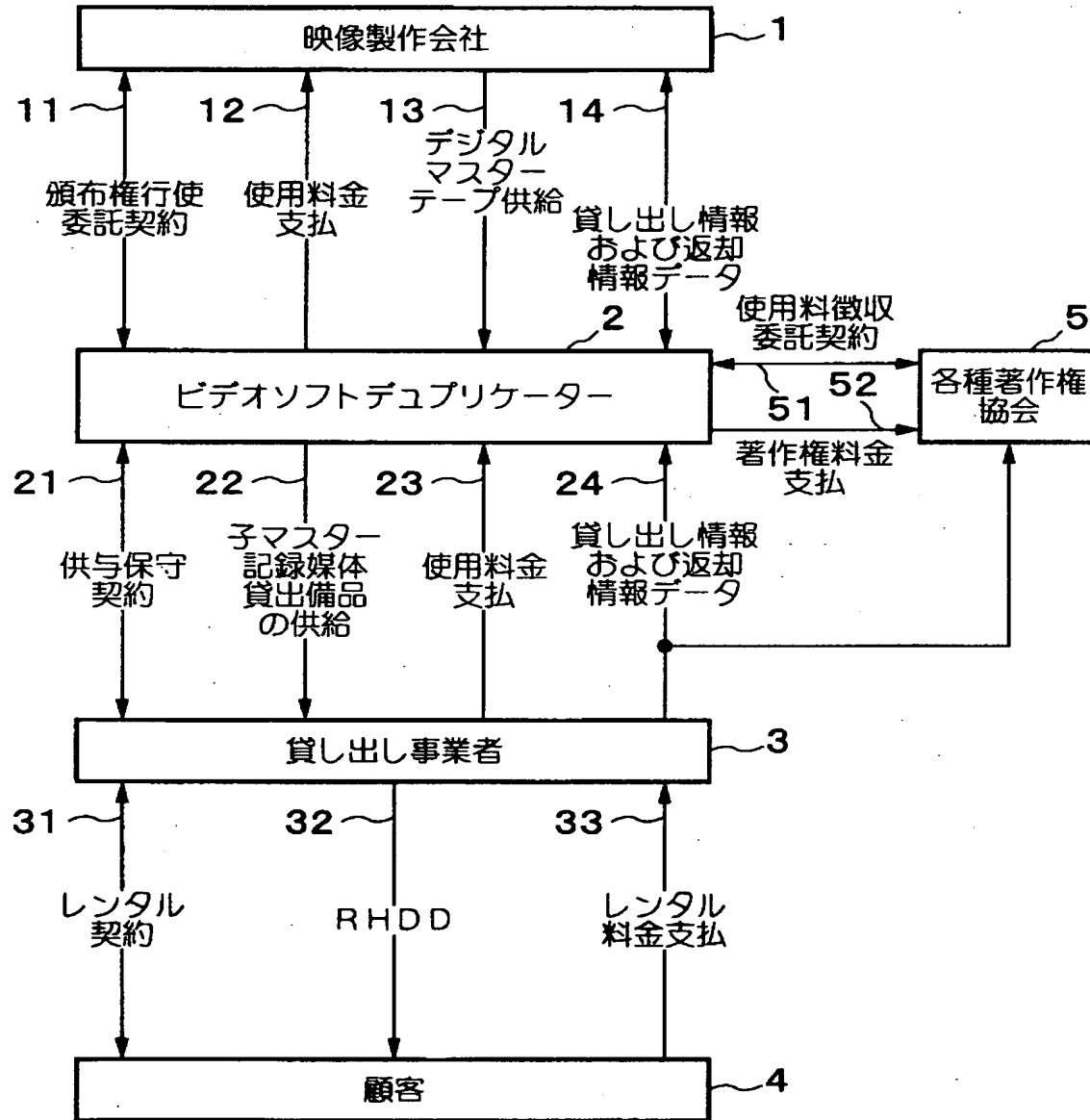
【符号の説明】



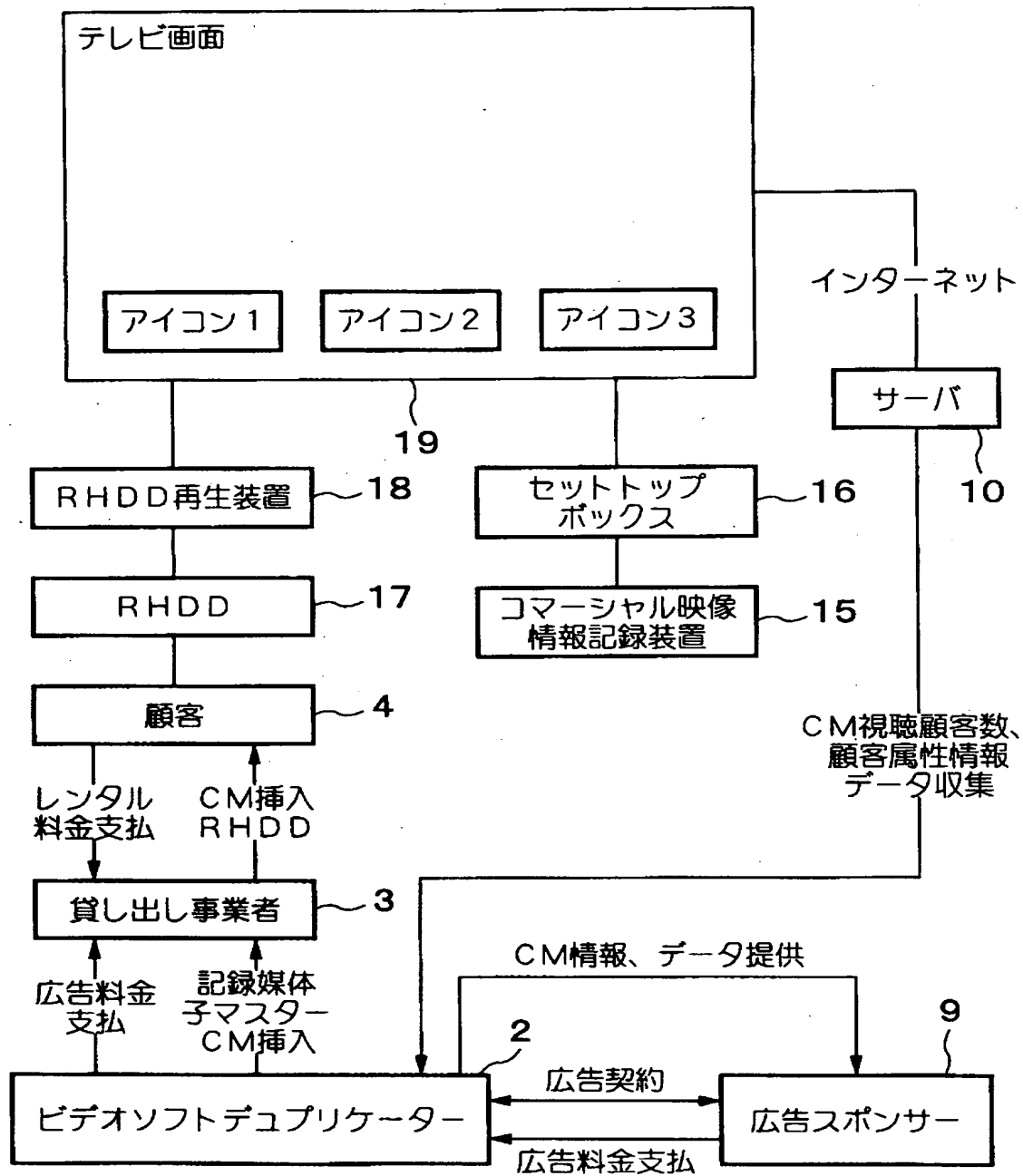
- 1…映像製作会社
- 2…ビデオソフトデュープリケーター
- 3…貸し出し事業者
- 4…顧客
- 9…広告スポンサー
- 10…サーバ
- 15…コマーシャル映像情報記録装置
- 17、17a～17e…RHDD
- 18、122…RHDD再生装置
- 101…コンテンツ格納部
- 102…制御部
- 104…揮発性メモリ
- 105…コンデンサ
- 106…サーバ
- 107…暗号復号部
- 108…再生部
- 109、119…タイマ
- 121…サーバ
- 160…管理センタ
- 162…サーバ
- 164…ネットワーク
- 166…コンテンツ記録媒体
- 167…ICカード
- 701…店舗サーバ
- 702…センタサーバ
- 703…インターネット
- 704…RHDD
- 705…再生装置

【書類名】 図面

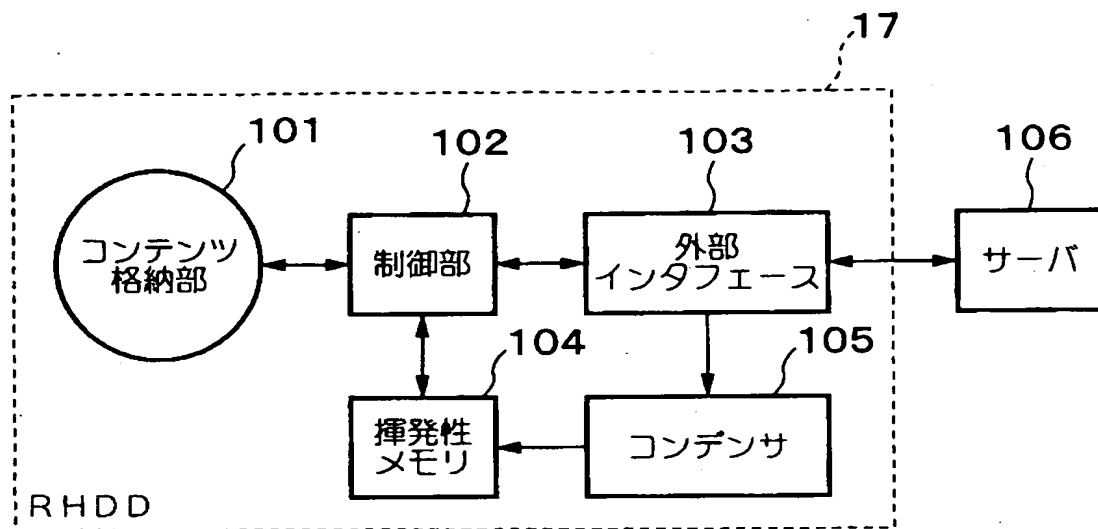
【図 1】



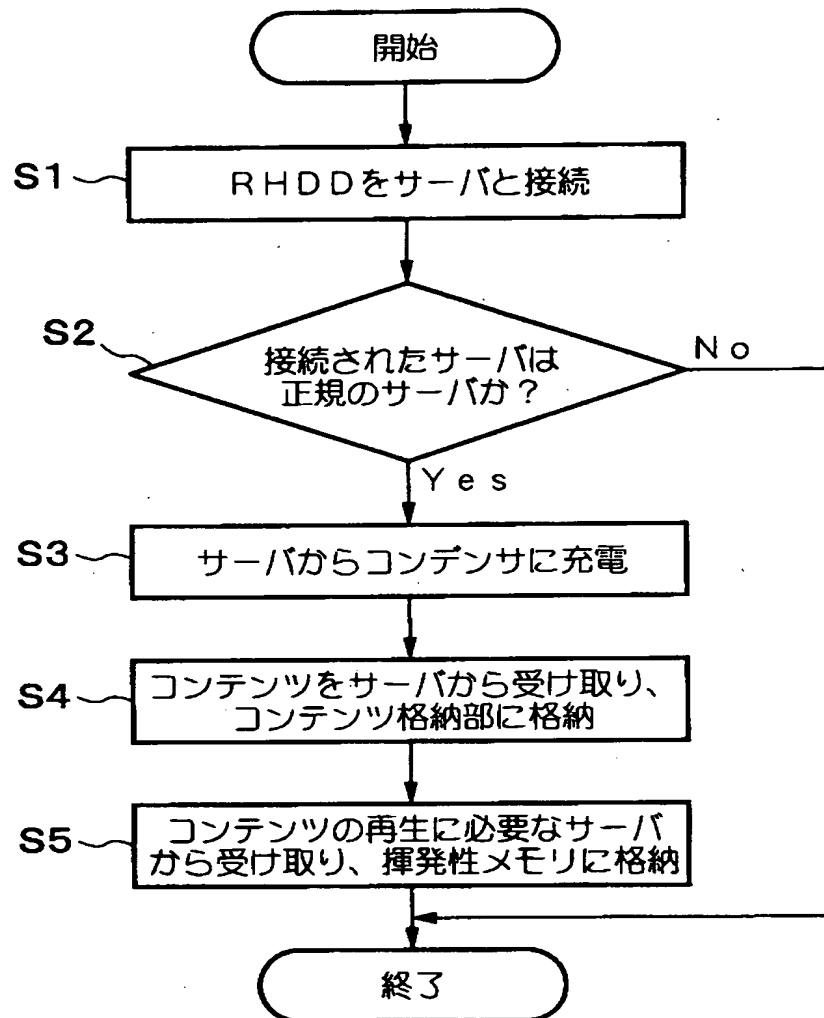
【図2】



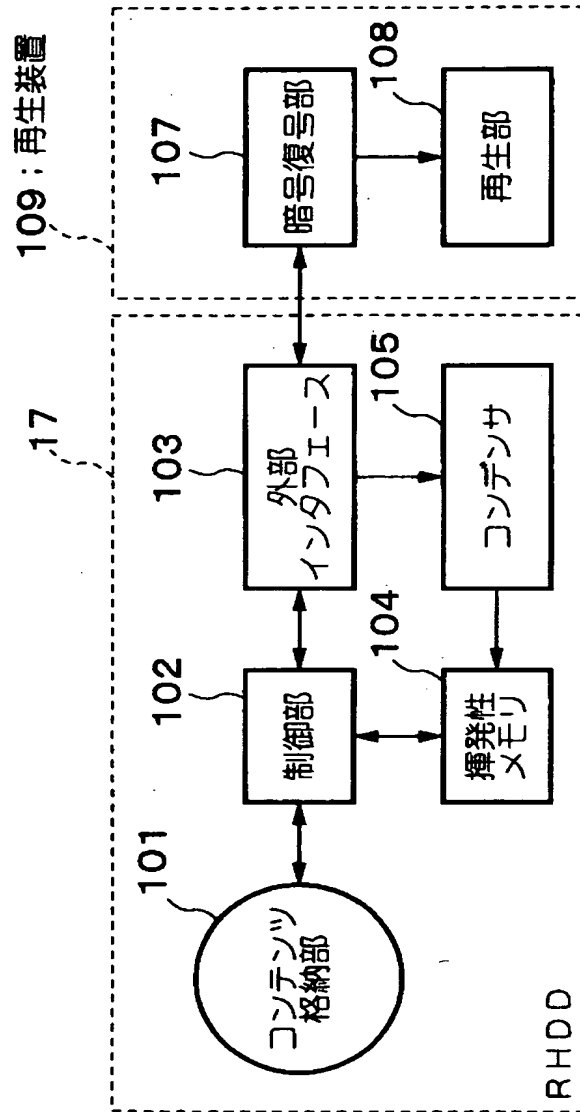
【図 3】



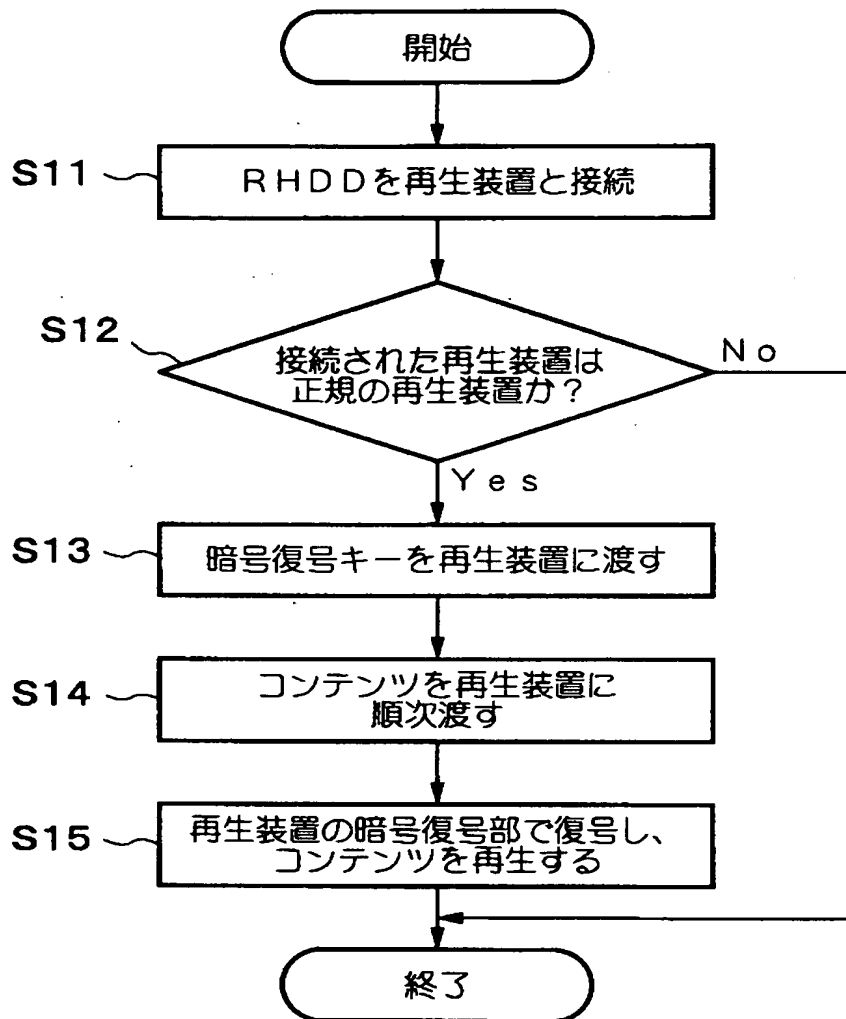
【図 4】



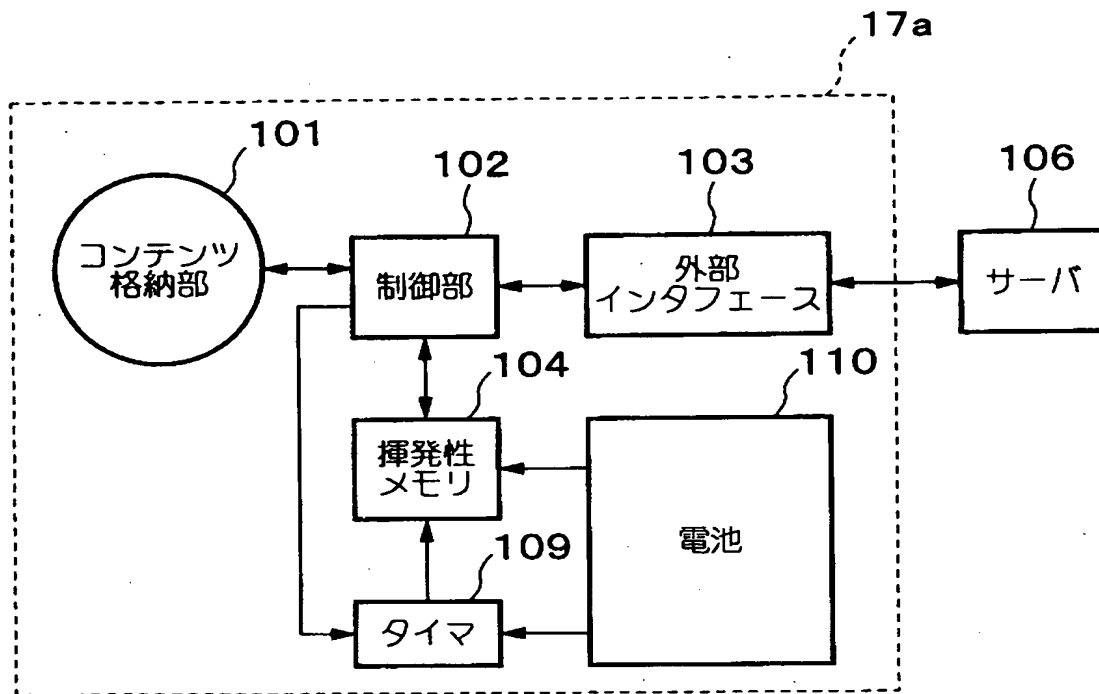
【図 5】



【図 6】

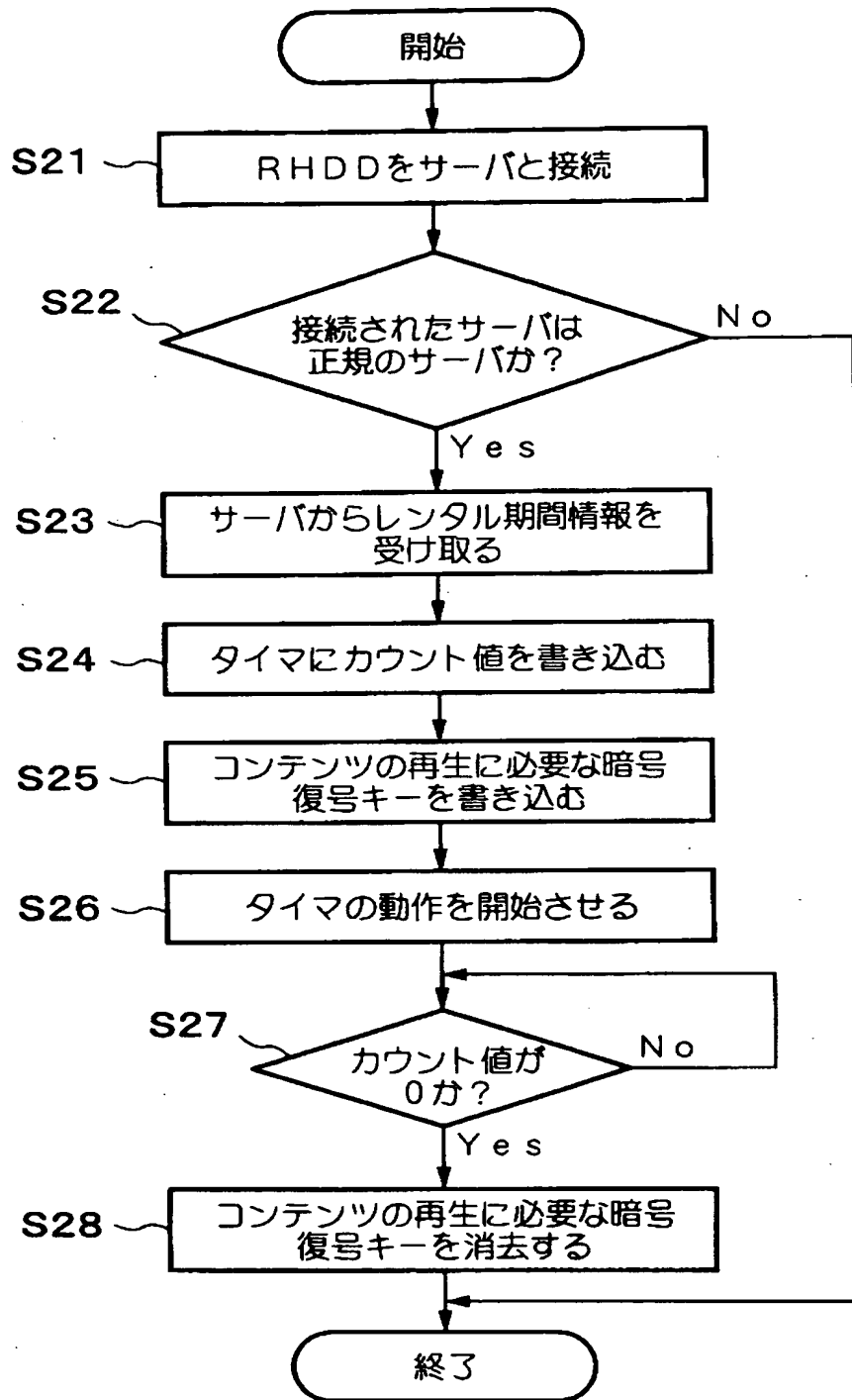


【図 7】

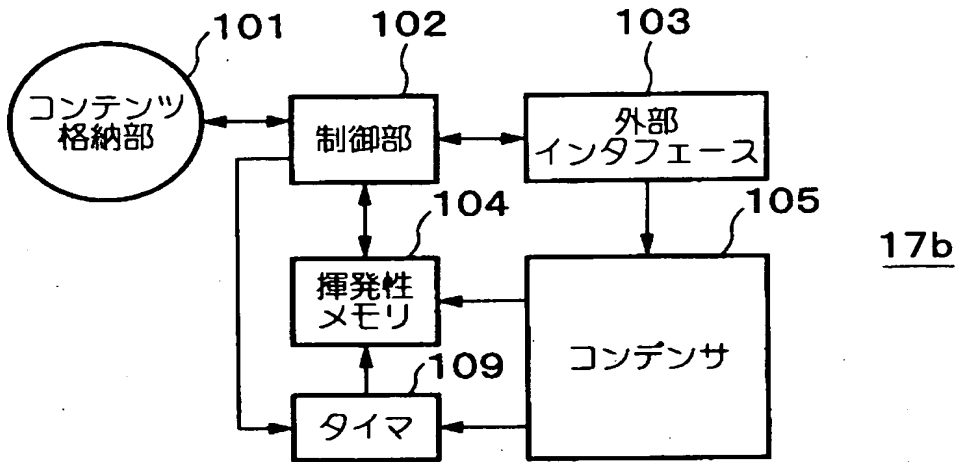




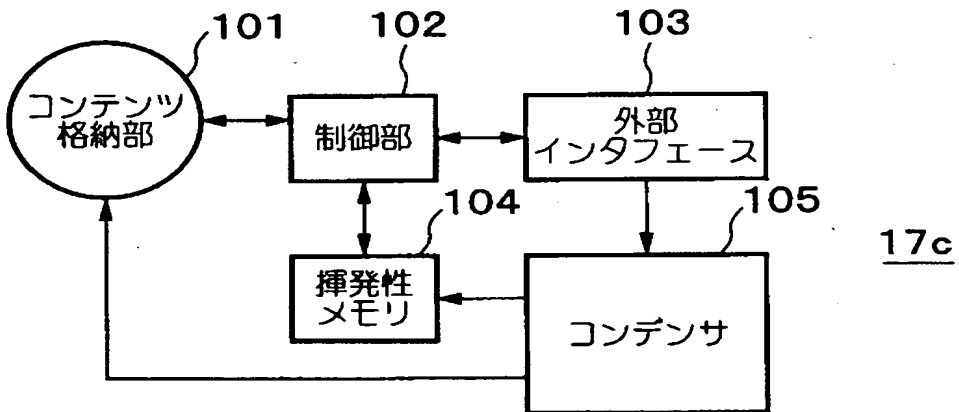
【図 8】



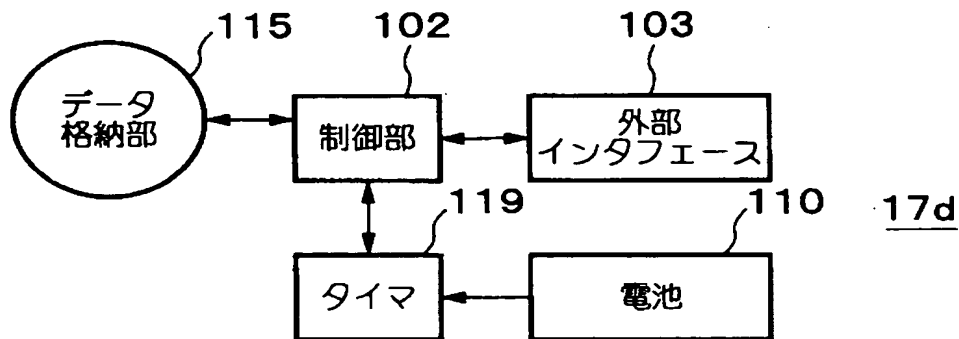
【図 9】



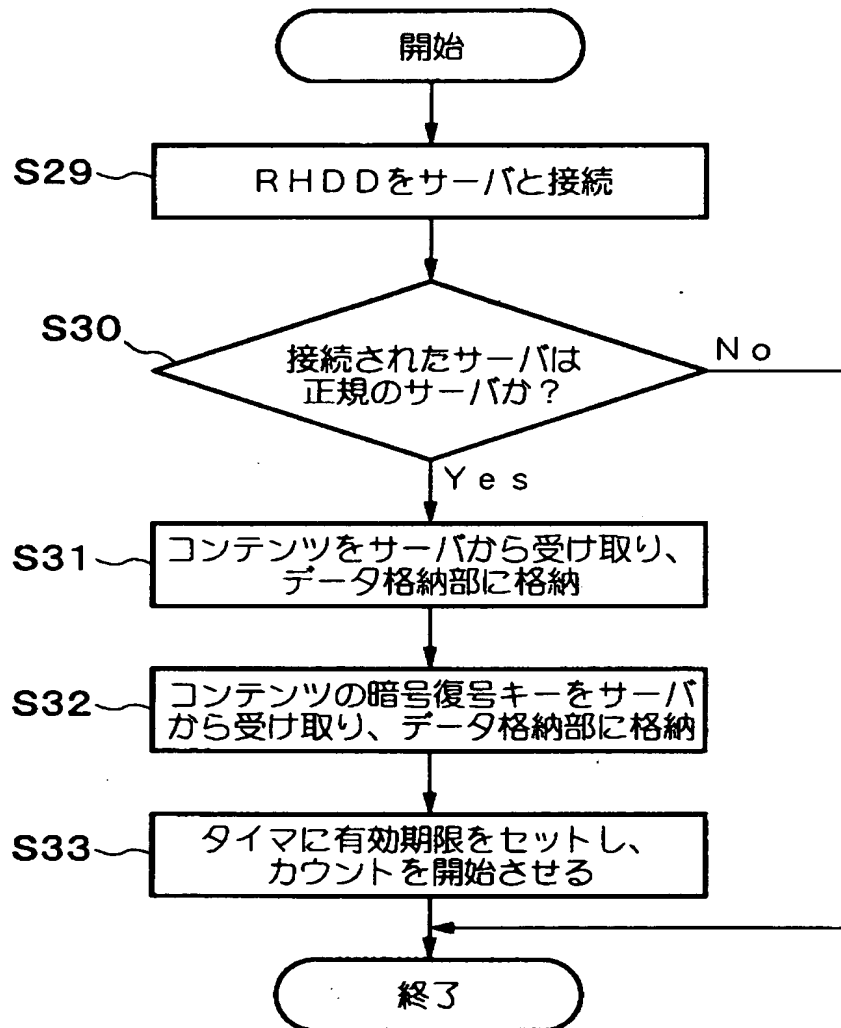
【図 10】



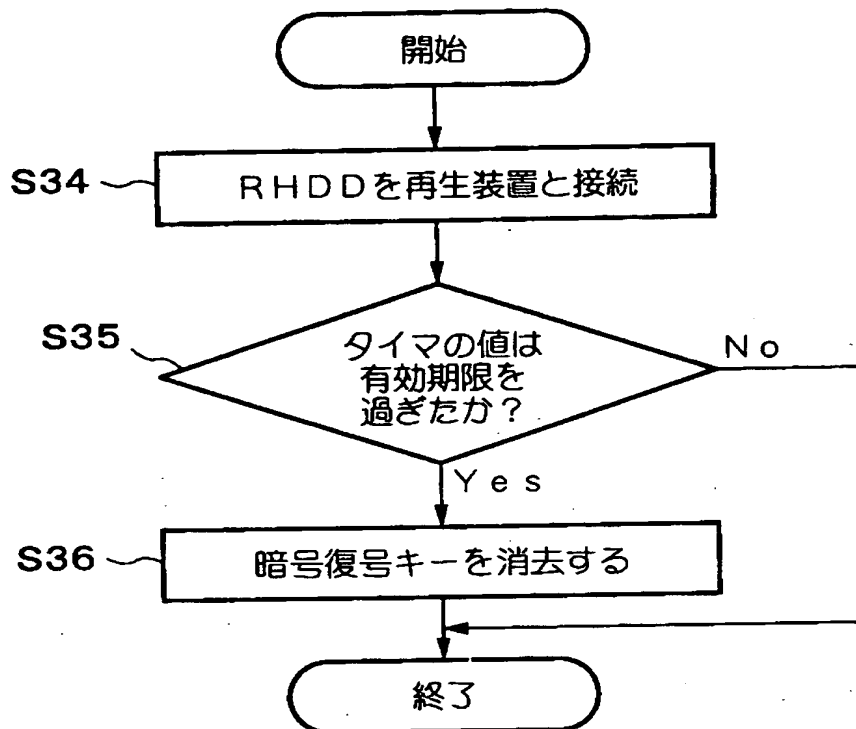
【図 11】



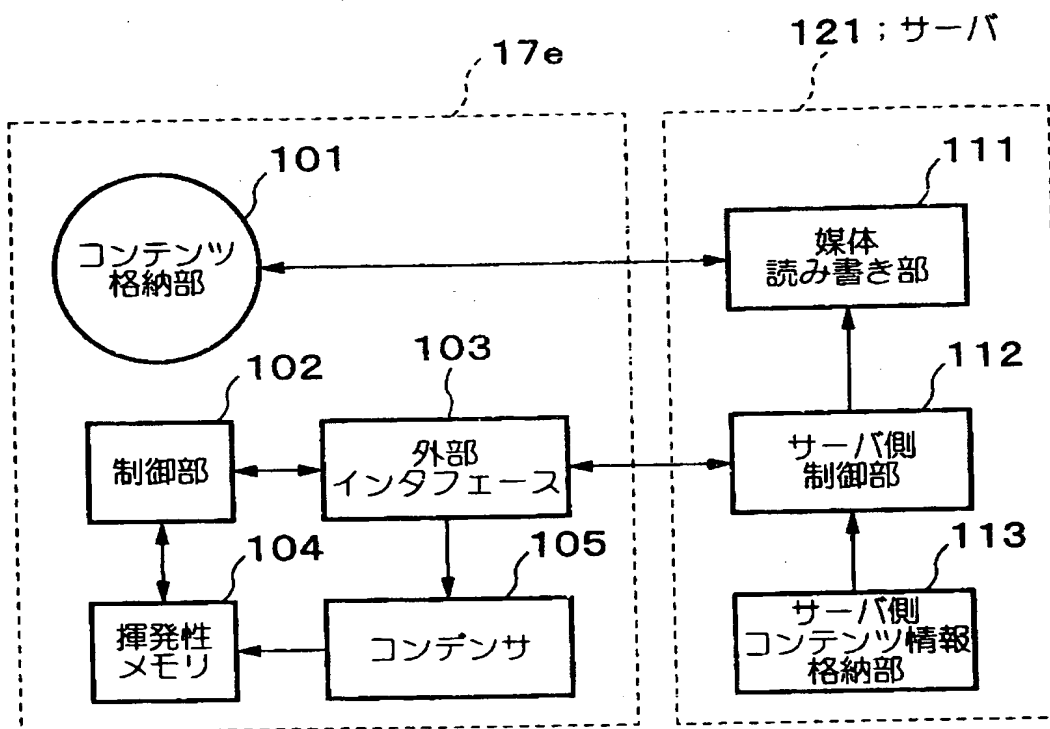
【図12】



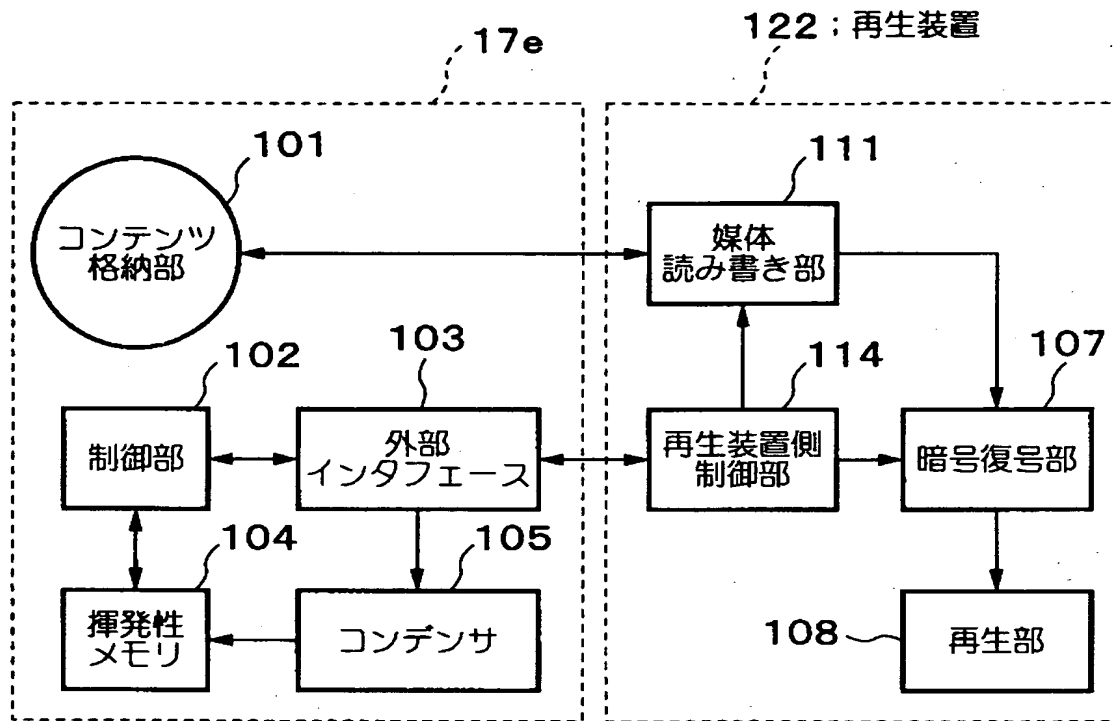
【図13】



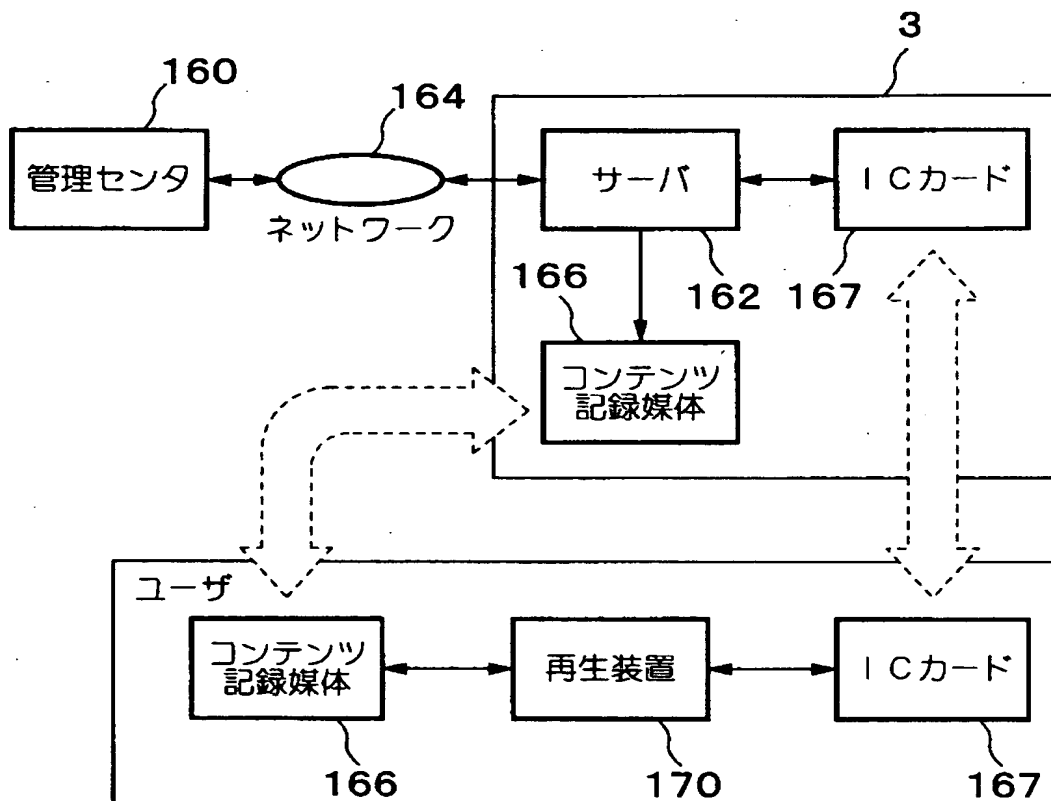
【図14】



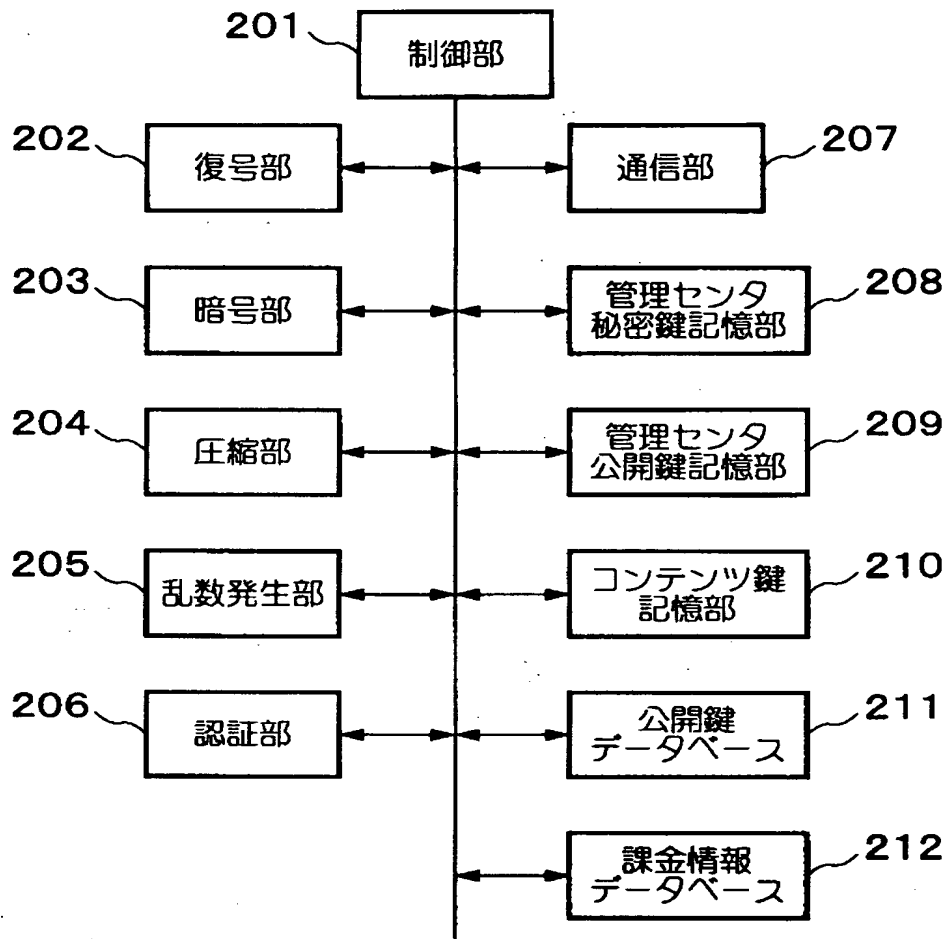
【図15】



【図16】

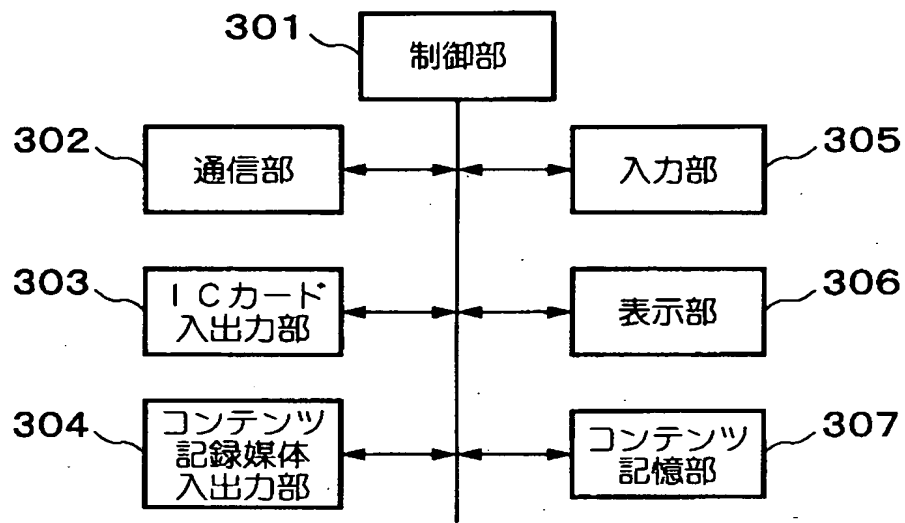


【図 17】



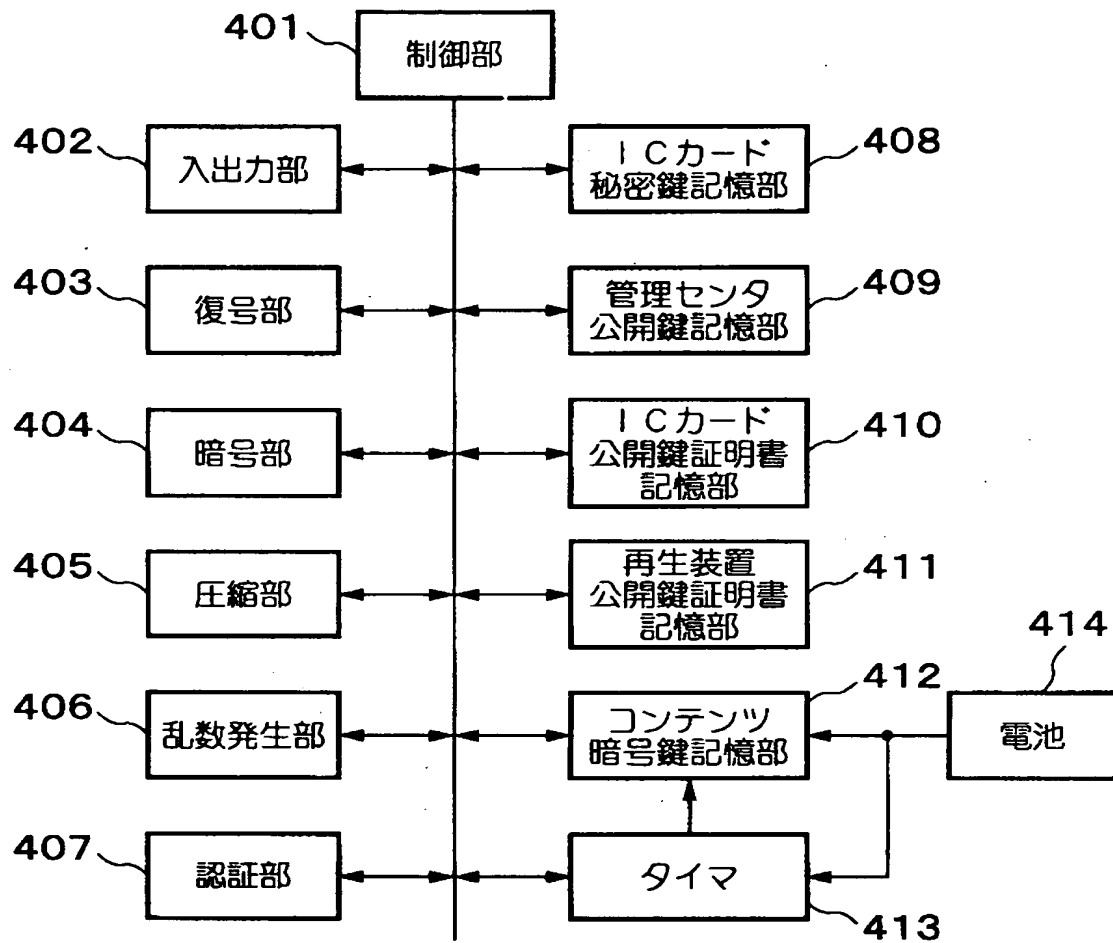
管理センタ 160 構成図

【図 1 8】



サーバ 1 6 2 構成図

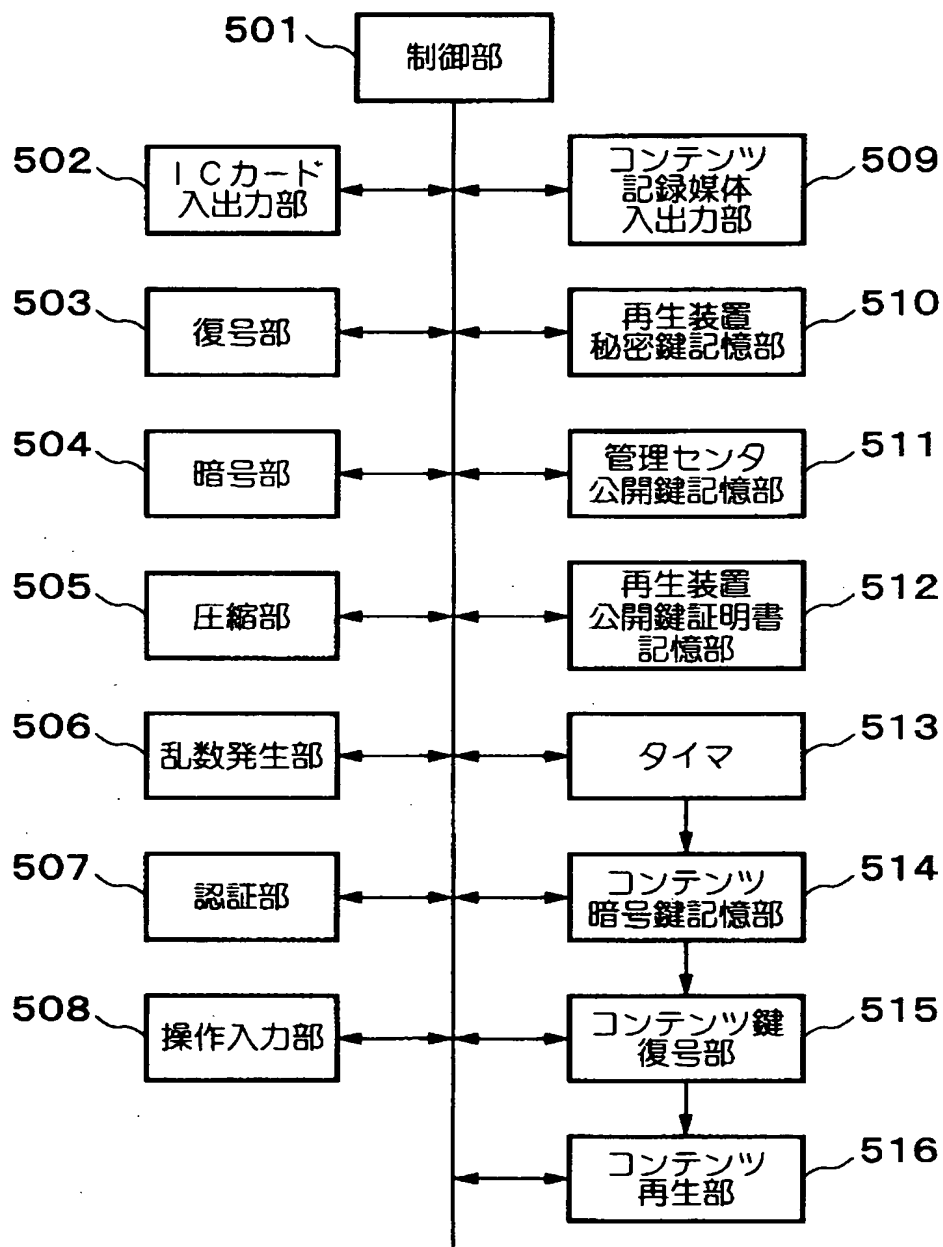
【図 19】



ICカード 167 構成図

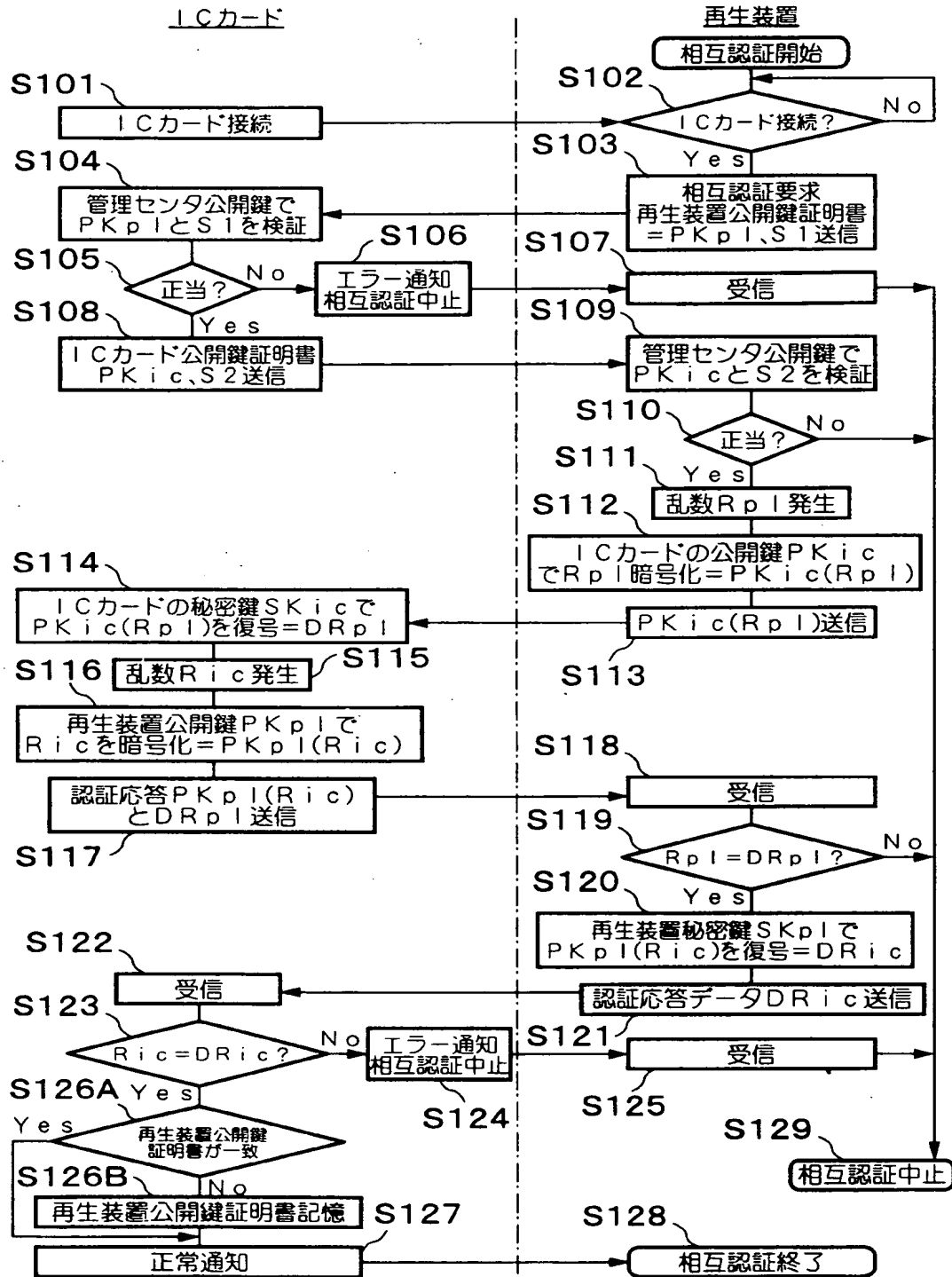


【図 20】

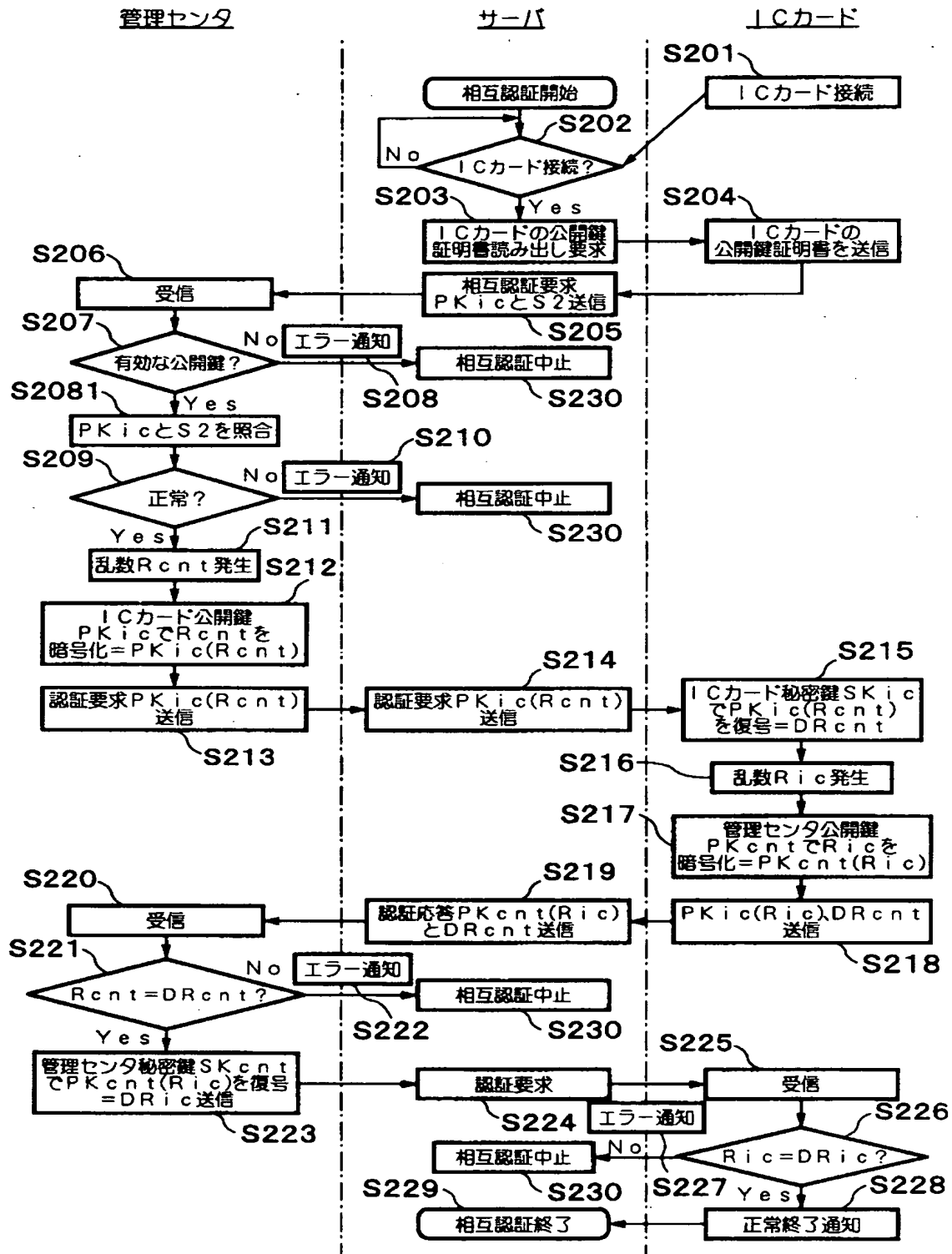


再生装置 170 構成図

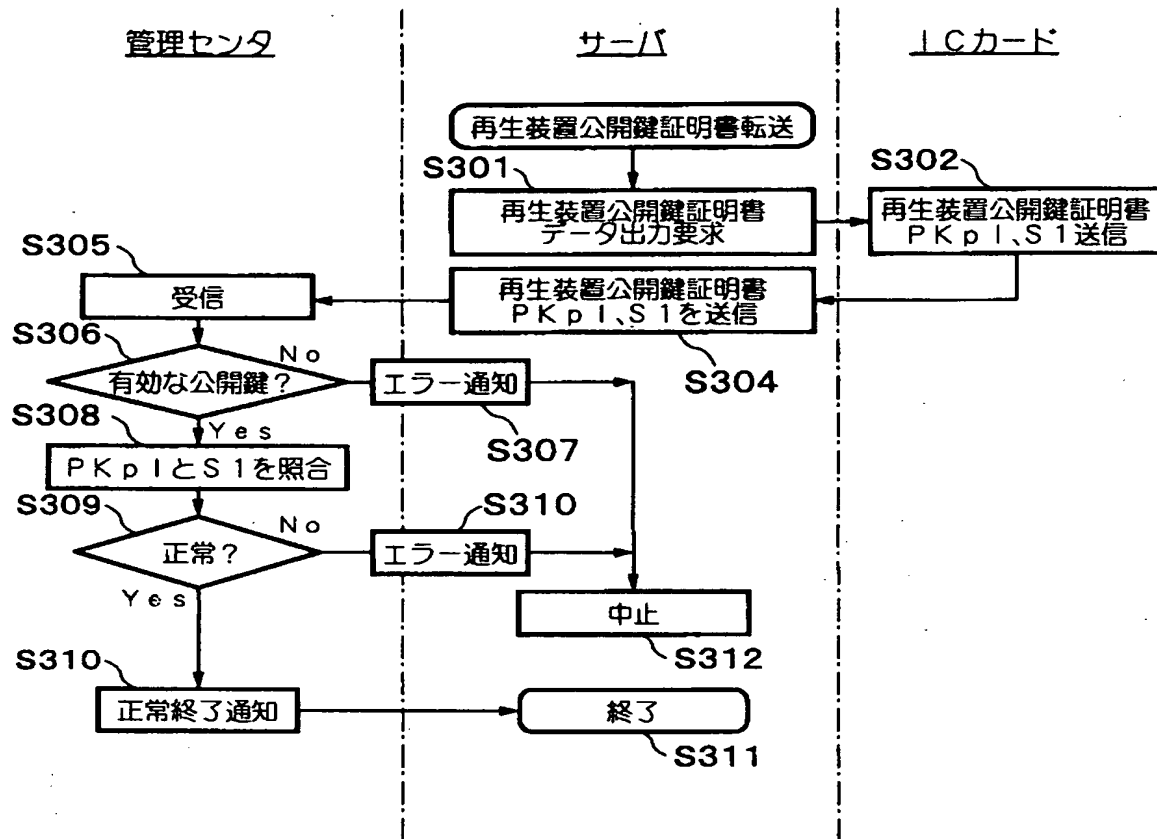
【図 21】



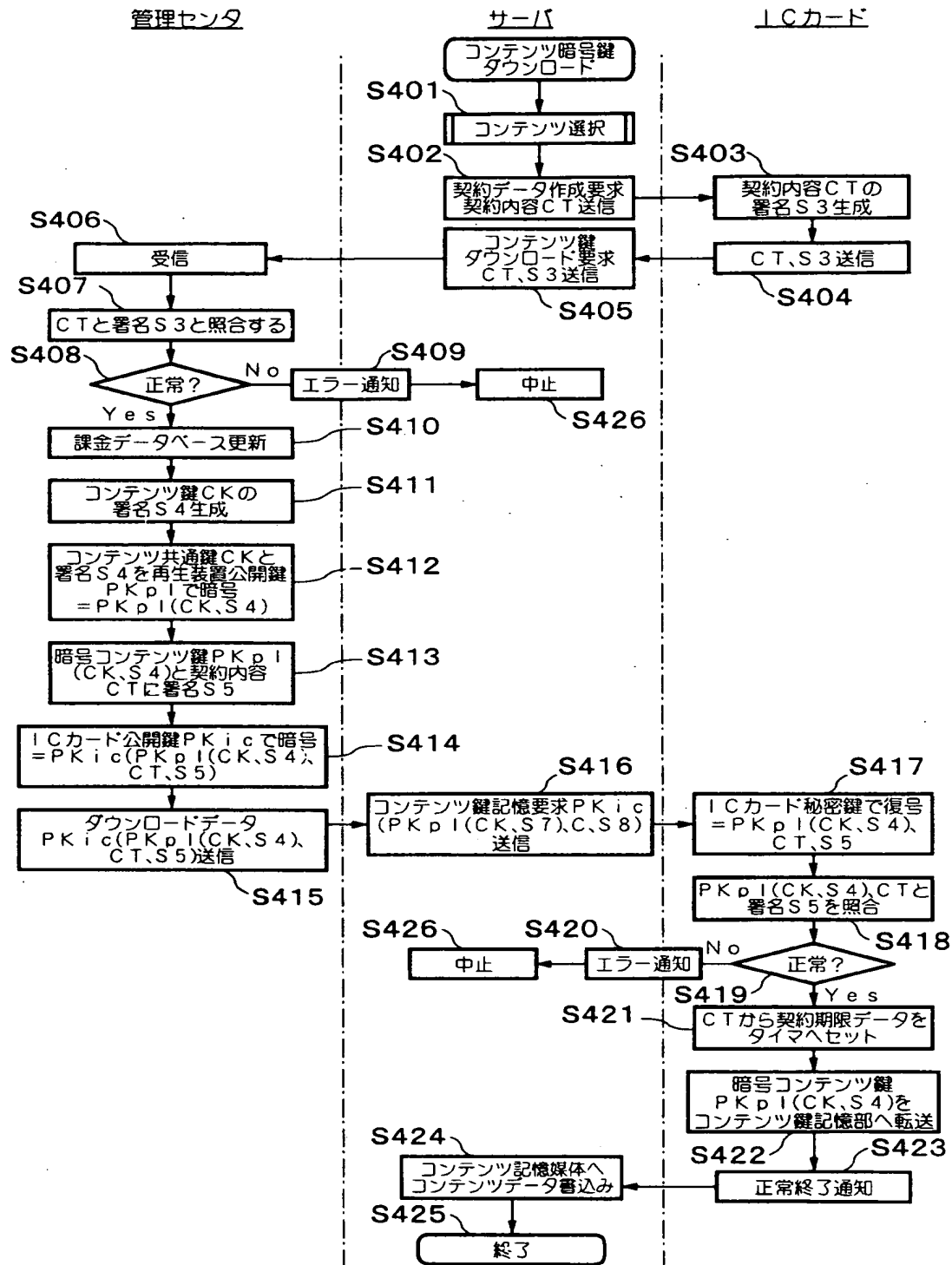
【図 22】



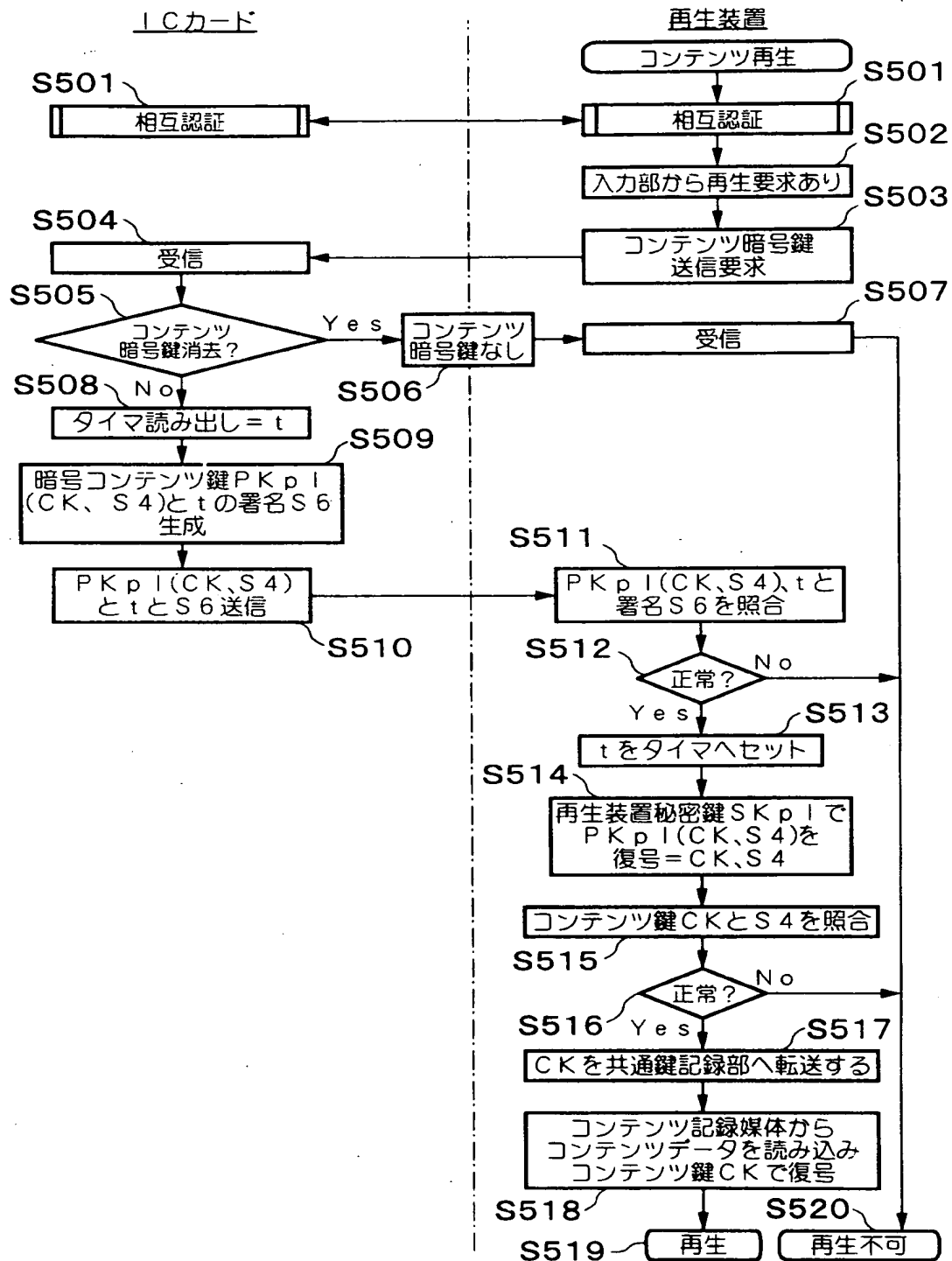
【図 23】



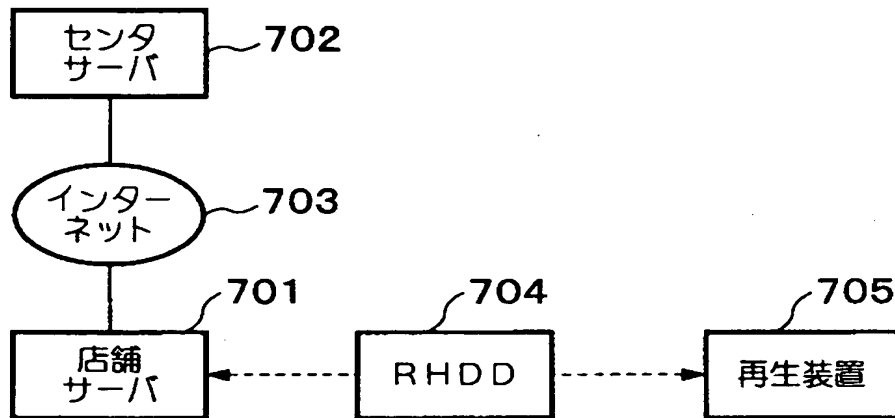
【図 24】



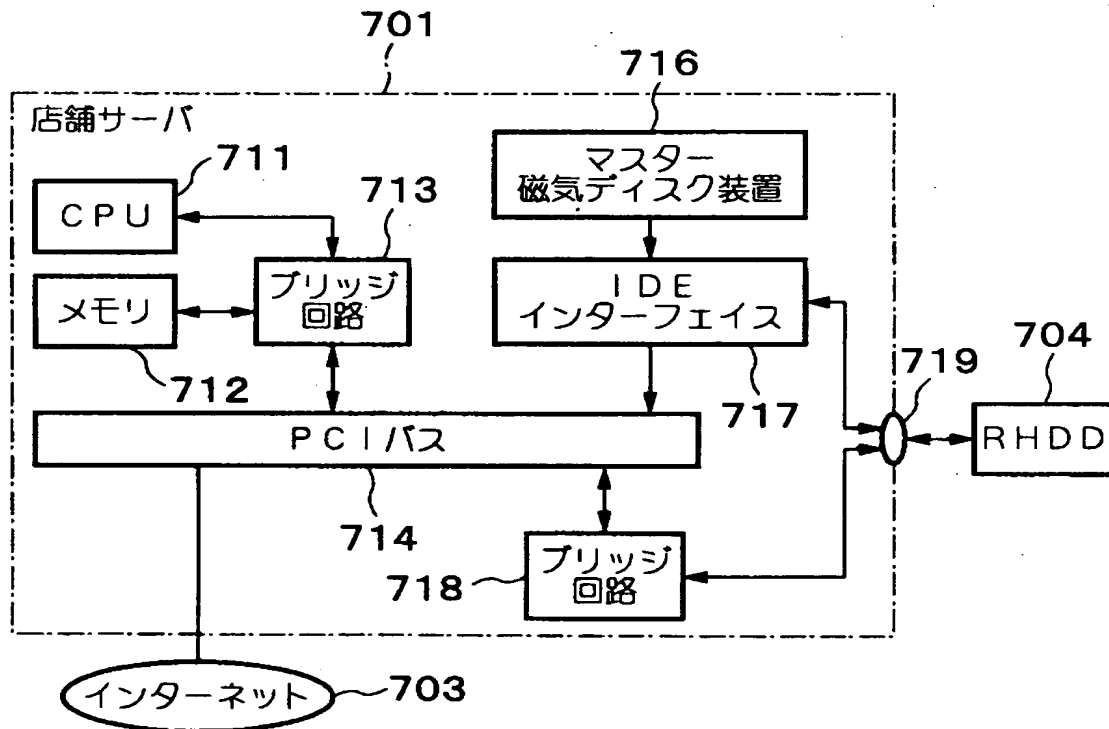
【図 25】



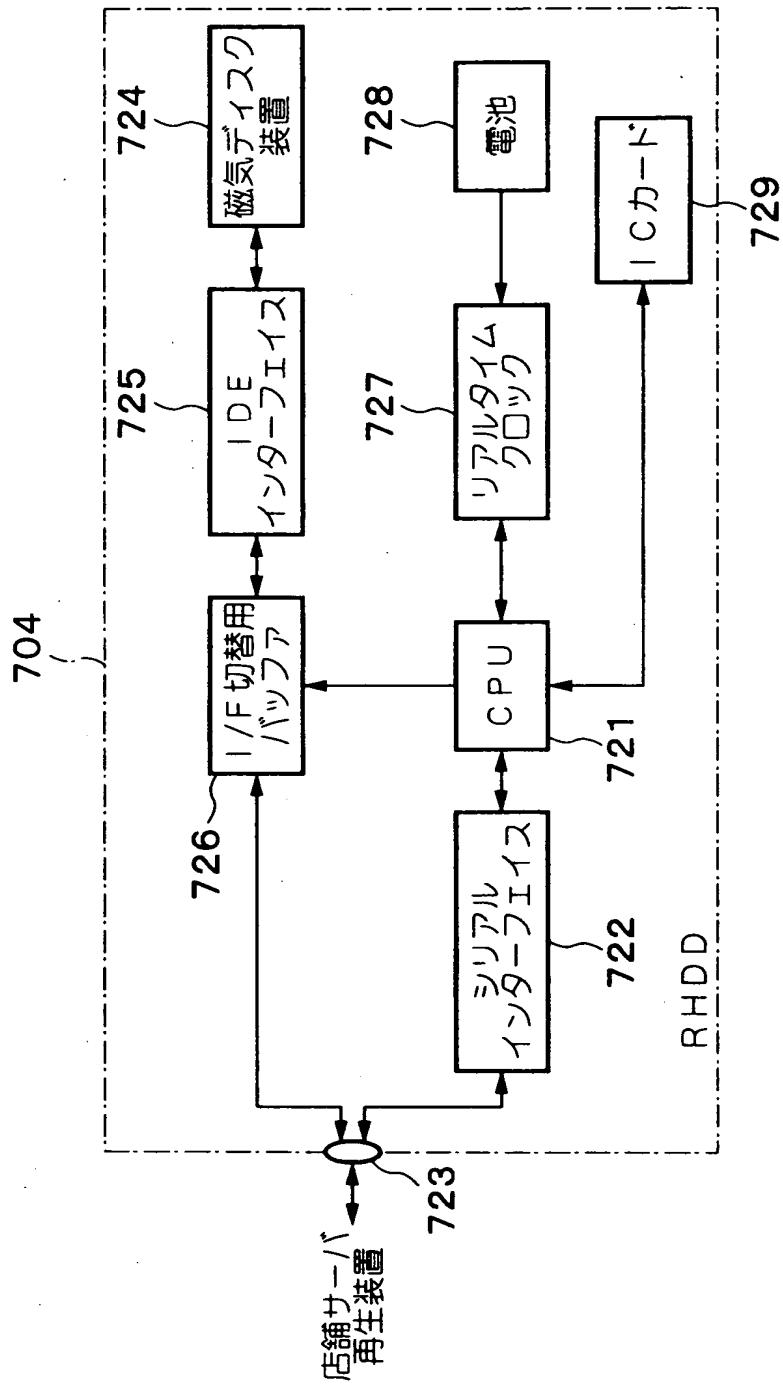
【図 26】



【図 27】

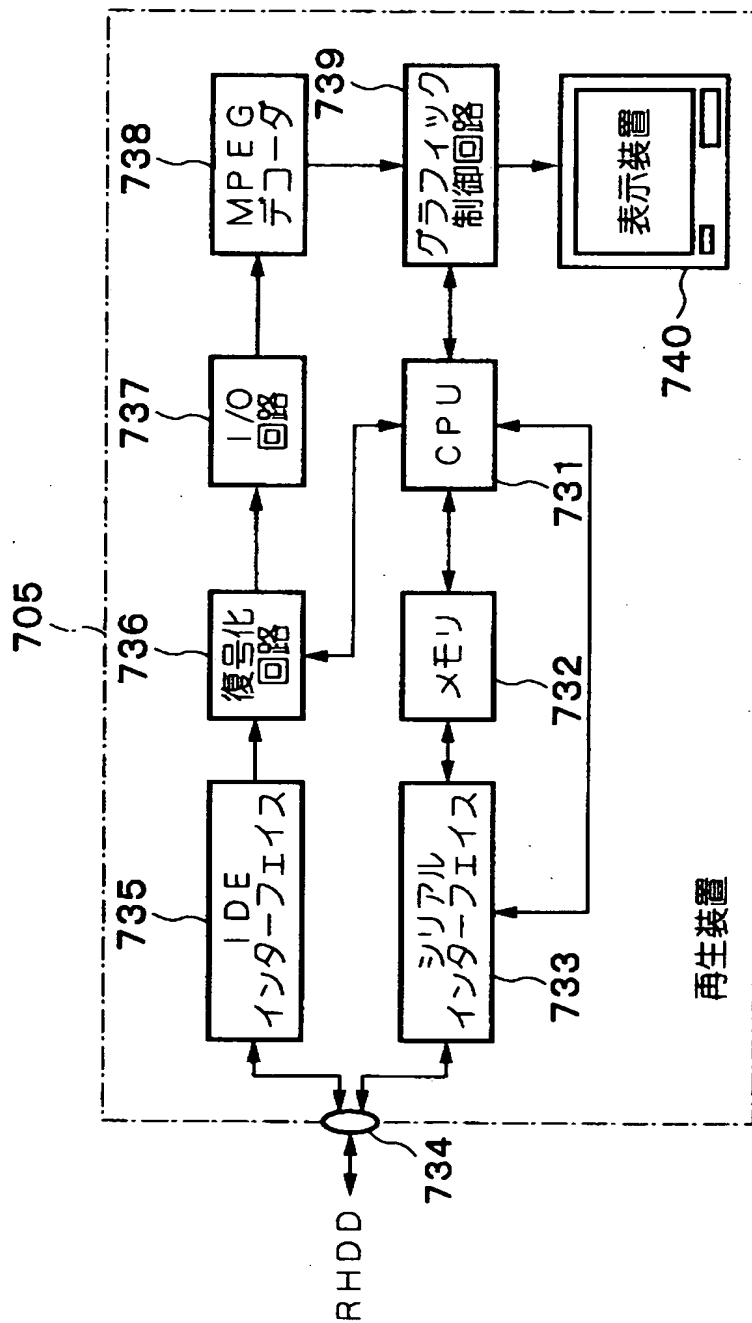


【図28】

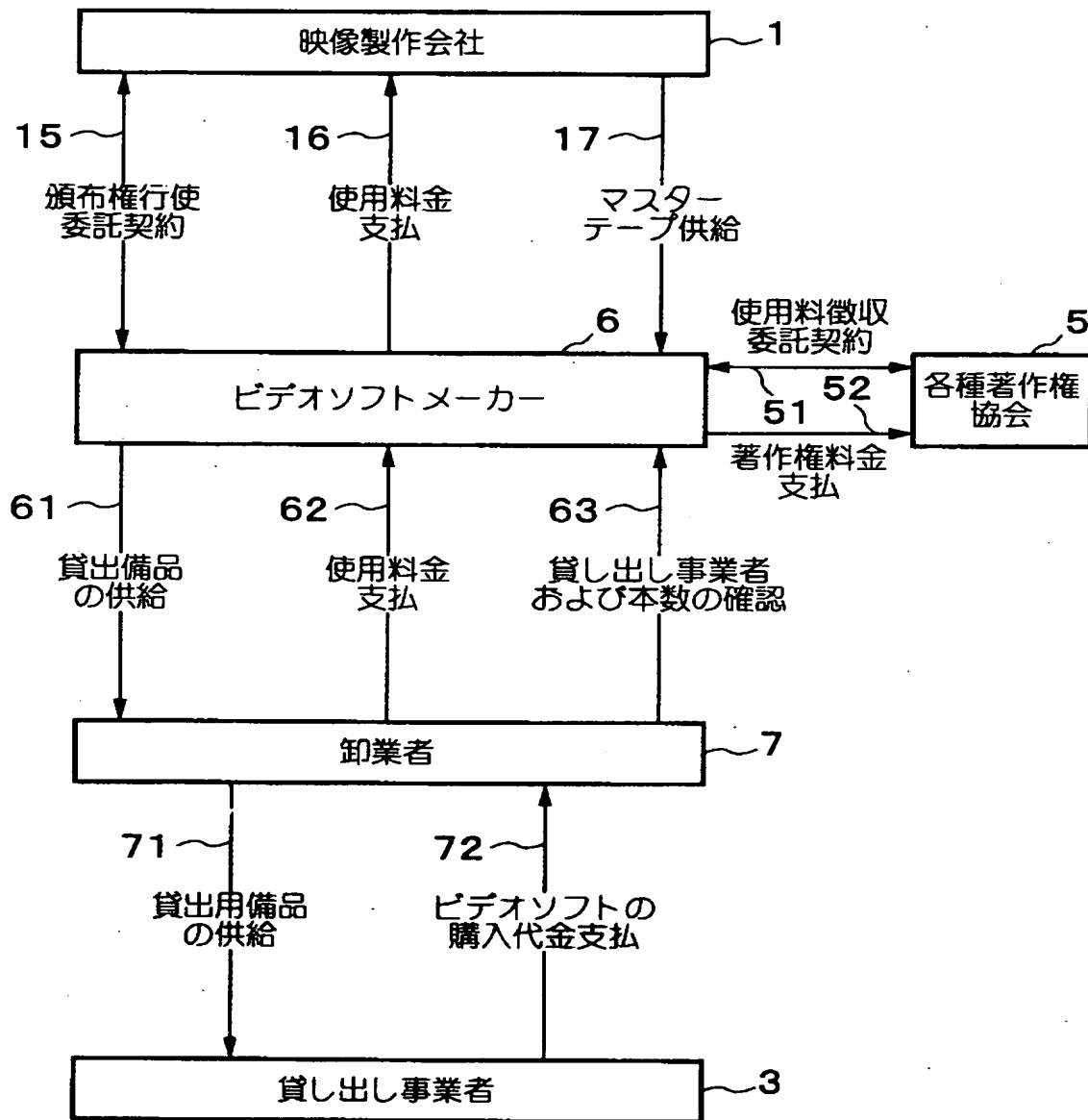




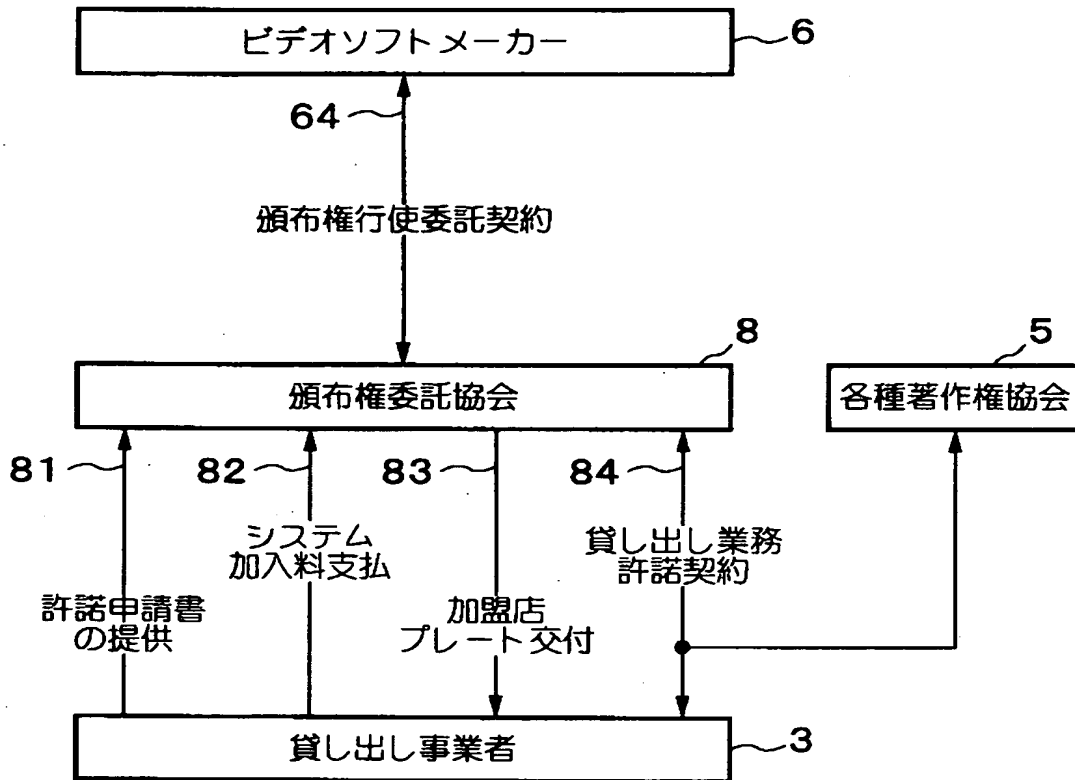
【図29】



【図 30】



【図 3 1】



【書類名】 要約書

【要約】

【課題】 貸出業者において不良在庫や機会喪失の虞れがないコンテンツレンタルシステムを提供する。

【解決手段】 映像製作会社 1 は、映像マスターを作成する。ビデオソフトデュープリケーター 2 は、映像製作会社 1 から供与された映像マスターから子マスター記録媒体を複製し、また、子マスター記録媒体の管理を行う。貸し出し事業者 3 は、ビデオソフトデュープリケーター 2 から分配された子マスター記録媒体に基づいて持ち運び可能な記録媒体（リムーバブル型磁気ディスク媒体；RHDD）を製作するダウンロード専用のサーバ端末を備え、希望する顧客にRHDDを貸し出す。また、貸し出した時と引き取ったときとの期間計算と、貸出料金を計算して、顧客から貸出料金の徴収を行う。顧客 4 は、一般貸し出し用のRHDDを、貸し出し事業者 3 から借り受け、再生装置によって再生する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願2001-013815
受付番号	50100083665
書類名	特許願
担当官	末武 実 1912
作成日	平成13年 1月29日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000004237
【住所又は居所】	東京都港区芝五丁目7番1号
【氏名又は名称】	日本電気株式会社

【代理人】

申請人

【識別番号】	100108578
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビ ル 志賀国際特許事務所

【氏名又は名称】	高橋 詔男
----------	-------

【代理人】

【識別番号】	100064908
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビ ル 志賀国際特許事務所

【氏名又は名称】	志賀 正武
----------	-------

【選任した代理人】

【識別番号】	100101465
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビ ル 志賀国際特許事務所

【氏名又は名称】	青山 正和
----------	-------

【選任した代理人】

【識別番号】	100108453
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビ ル 志賀国際特許事務所

【氏名又は名称】	村山 靖彦
----------	-------

次頁無

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日  
[変更理由] 新規登録  
住 所 東京都港区芝五丁目7番1号  
氏 名 日本電気株式会社